A 10-step plan for disaster recovery in the digital age

With everything you need to know from auditing and testing your systems to considering the impact of mobile and cloud services, this guide will help you prepare your organisation to face the challenges of the digital future.
Modern workplaces are more accessible than ever before. It’s becoming standard practice for employees to work from anywhere, connecting to their office environments through mobile devices and cloud services.

But this accessibility comes with a risk of disruption to your business, and a responsibility to manage and mitigate that risk. If your critical systems and applications suffer outages, you could be left in a vulnerable position – unless you have a disaster recovery (DR) plan that ensures business continuity.

That’s why we’ve created this DR guide. It’s a simple 10-step plan to help you keep on delivering services to your customers and staff, no matter what drama the digital age throws at you.
The 10-step guide to disaster recovery in the digital age

1. Get to know your risks
2. Stress test your systems
3. Consider the cloud and mobile impact
4. Give your gatekeeper more power
5. Build in redundancy
6. Develop a detailed DR strategy
7. Be agile
8. Take an executive approach
9. Constantly talk with your people
10. Ask the experts
1. Get to know your risks

There’s no one-size-fits-all approach to DR, because every business is unique. And it’s difficult to get where you need to go if you don’t know where you are right now.

A systems audit lets you step back and view your current operating environment and roadmap, so you can understand your risks and vulnerabilities.

Start by making a list of the disasters, failures and faults that might affect your organisation, and the impact they would have on your systems, operations and customers. In addition to security (cyber attack, malware, viruses) and technical problems (power outages, hardware failures), triggering events can also include environmental, political, or human factors:

- What would happen if protests prevented access to your offices?
- What if localised flooding took your primary data centre offline?
- What if your team caught the flu and couldn’t work for two weeks?
- What if weather caused prolonged, widespread power outages?
- What if someone opened an email attachment that turned out to be ransomware?
- What if a member of your team accidentally deleted critical data?

Each of these scenarios could disrupt a different set of local and remote systems, with different flow-on effects throughout your business. But your customers will see the same result: downtime.

How long will it take you to restore services, and how much downtime can your business tolerate?

Tip
If external vendors manage or host your applications and data, review your service level agreements (SLAs) to learn precisely where you stand in the case of outages or downtime.
2. Stress test your systems

Every minute of systems downtime is a potential loss for your business – lost sales, lost productivity, lost goodwill. Depending on your industry, you may also face regulatory or contractual penalties. It’s critical to understand how much downtime you’re dealing with, and where you are most vulnerable.

Thorough testing will help you identify which critical applications are most likely to fail and how long it will take to bring them online again.

A sandbox environment creates a safe testbed where you can simulate a disaster event, practise bringing your systems back online and identify any chinks in your armour. Pay close attention to your authentication tools and your data storage, backup and recovery plans, as these are often central to all DR efforts.

With your system testing complete, you should be in a better position to prioritise different elements of your DR plan.

However, it’s an involved process and it needs to be done right. So if you don’t have the time and the budget to get it done in-house, consider hiring an expert contingency engineer to assist. They’ll have experience working with a range of business systems and applications, and can handle the bulk of the testing while you focus on the business aspects of DR.
3. Consider the cloud and mobile impact

Cloud platforms & mobile devices have become a part of our everyday lives. We use them to keep in touch with friends and to follow what’s happening in the world. We even use them to be more productive at work – we can connect to enterprise systems from anywhere in the world at any time.

But as our cloud and mobile dependence increases, so too does the complexity of securing corporate data and systems while providing flexible and responsive IT services to match our users’ expectations.

This is even more true if your IT policy includes a Bring Your Own Device (BYOD) option. By allowing corporate data to be stored on personal computers and mobile devices alongside file sharing and social media apps, you’re increasing the risk of data loss through human error or an unknown vulnerability.

A common reaction is to completely lock down your systems. But unless you can rapidly respond to new software requests, this often leads to user frustration and creative workarounds. (Who hasn’t seen an employee take a photo of a printed file?)

Some organisations opt for the other extreme, enabling users to install their own software. Months or years later, they find a proliferation of apps and storage solutions.

So if you haven’t already, review your IT, BYOD and social media policies and ensure everyone is adequately trained. Then go on to review all the apps used in your organisation, and plan how you will select and migrate to a standard set.

The discovery process can be difficult, especially if you don’t have 100% visibility of user devices. Further to that, staff may be reluctant to give up the tools they know and love. It’s common to encounter resistance, but it might help to point out you can only provide DR if you know about these services.

---

**Tip**

Users generally have a good reason for selecting and installing apps, so it makes sense to work with them to find a solution that works for everyone.
4. Give your gatekeeper more power

There’s a good chance your organisation is already using mobile device management (MDM) to reduce the risk and potential impact of malicious or accidental data loss. MDM platforms usually include tools to install certificates, enable or disable native device capabilities, remotely lock or wipe devices, and provide access to a Virtual Private Network (VPN).

You’re probably also connecting laptop computers, printers and maybe even point of sale terminals to your network’s routers and switches, so they also present a risk. An Identity Services Engine (ISE) works similarly to MDM, allowing you to create and enforce security policies for all endpoint devices on your network.

To boost your gatekeeping power, you’ll also want a traffic monitoring system – one that can watch what’s passing through your firewalls, routers and switches.

An Intrusion Detection System (IDS) sits alongside the network, analysing traffic at multiple points to identify anything that looks out of the ordinary that could signal a policy violation, configuration error or information leak. Alerts from an IDS warrant further investigation by your security team.

An Intrusion Prevention System (IPS) also sits inline with the network, guarding entry points and scanning all incoming traffic to enforce its collection of rules. Where a firewall only passes known “good” traffic that meets certain conditions, an IPS will only drop known “bad” traffic.

Each of these systems will help you monitor your network and reduce the risk of data loss, but only if paired with business policies and procedures that enable your IT department to respond quickly to threats.
5. Build in redundancy

Redundancy has always been an essential element of DR, and one that used to be complex and costly to ensure for all critical systems. Physical DR infrastructure needed to be regularly maintained, upgraded and replaced – a significant capital expenditure.

But the rapid advancement of cloud platforms and managed service solutions has made it easier and cheaper to maintain additional servers and systems and to deploy additional resources as required. Whether you’re using Software as a Service (SaaS) for licensing and updates of key systems, or Infrastructure as a Service (IaaS) to deploy your entire corporate network in a virtualised environment, you’re simplifying your DR strategy.

The model of distributed resources and high degree of virtualisation used by most cloud service providers means that redundancy is now built into the architecture. If there’s a problem with one of your virtual servers, simply spin up another one. If you’re running out of disk space, assign more. And if your cloud vendor’s hardware fails, you should automatically failover to another location.

The DR benefits of cloud services have been proven, but if you choose to build your own redundancy solution instead, be sure to research current best practices.
6. Develop a detailed DR strategy

Now you’ve thought about everything you might need to minimise and manage the damage of data loss or system outages, it’s time to build your complete DR strategy.

While your complete IT strategy will focus on the products and services your team delivers to the business, your DR strategy needs to take a wider view, considering roles and responsibilities beyond the IT department.

Ask yourself:

- Who is responsible for declaring that a disaster has occurred and that the DR plan should be enacted?
- Who will manage the disaster recovery operation?
- Which staff members are considered critical for business continuity?
- Who is responsible for communicating with your staff, customers, investors and the press about the changing situation?
- Will you require additional level 1 support resources to handle customer enquiries?
- Which elements of your DR plan will be performed by third parties, and which by staff members?
- Who is responsible for maintaining the DR strategy and ensuring it is updated as your operating environment changes, at least annually?
- How will you train your staff to ensure DR preparedness?

Drawing up your strategy is likely to be both time-consuming and challenging, but if you focus on the big picture and centre your plan on avoiding the greatest potential losses, it’s well worth the investment.

It’s impossible to foresee everything that might go wrong at the outset, so we recommend you put your DR plan to the test, too. DR drills are just like fire drills for your key systems, networks and databases.
7. Be agile

As technology evolves, so do the threats to your business. To keep up, your DR plan needs to be agile, like your operating environment. It’s not enough to just prepare and test your DR strategy once – you need to update it each time there’s a change to your operations or your IT architecture.

It might sound like a lot of work, but it’s worth it. Would you really want to risk an out-of-date DR plan that might be worse than no plan at all? If you’re not 100% confident in your strategy, you’re likely to waste precious hours working on the wrong part of the picture, should the worst happen.

You can share this workload without simply assigning people to a change management team. Activities like dedicated problem-solving days or in-house hackathons are fun ways to foster a culture of innovation and continuous improvement.

Taking an agile approach is likely to create new opportunities in your organisation, too, with employees more likely to suggest new ways you can use technology. We’ve recently seen the blockchain boom, with potential applications beyond finance into industries ranging from biosciences to construction.

Who knows – your future IT architecture could incorporate quantum encoding and encryption as part of your DR plan!

Tip
Your suppliers, customers, colleagues and contemporaries share a wealth of experience you can draw upon to identify and prepare for challenges your organisation may face.
8. Take an executive approach

Executives are people who make things happen. Through insight and action, they lead others to a set objective. When you take an executive approach to disaster recovery planning, you’re building systems and processes to secure your future success.

When it comes to selecting systems, it’s easy to be seduced by bleeding edge technology – products and services that promise to be the next big thing but haven’t yet been proven in the practice. Your DR plan is not the place for early adoption. There are clear benefits to staying in the mainstream, such as better support from vendors and the industry, and greater stability.

Executives should also know their industries well and be familiar with best practice. Your organisation won’t be identical to others, but it will share similarities, so you can be guided by your peers’ and competitors’ strategies.

Finally, executives must understand each part of their organisation and how it fits into the whole. Demonstrating this knowledge in your DR planning will reassure others that you can effectively support them, and help you earn trust and respect from people throughout the organisation. They’ll be more willing to help if you need it – just another benefit of the executive approach.
9. Constantly talk with your people

There’s no doubt that the people you work with hold valuable information about your business processes and systems. In a DR scenario, it’s important to understand where all these people fit in. It’s also critical to know who has the skills and personal attributes to deal with the situation, and who may benefit from further training.

But have you thought about how they’re also a part of those systems?

Whether they are a salesperson entering customer order details, a procurement team member raising a purchase order, a manager onboarding a new staff member, or an IT professional configuring your network, they’re the human element of your systems. And they’re perfectly positioned to provide expert advice about those systems and give you early warning of any threats.

The easiest way to maintain this steady stream of information is to keep the conversation going. While a formal feedback process is always useful, a casual chat may allow for faster response.

Whichever approach you choose, be sure to recognise employees for their input, to show that you’re willing and ready to listen to their ideas.

Tip
If you’re having trouble connecting with other departments, use your marketing or internal communications people to help translate any technical jargon.
10. Ask the experts

Help can come in all shapes and sizes and from diverse sources. Not just from inside your business, either.

Your average big business knows this, and they outsource regularly. But smaller businesses may resist this approach, often because it’s perceived as expensive or unnecessary.

The truth is that outsourcing is often better value for money than doing it yourself. This is particularly true in any spaces where the cost of maintaining skills and equipment is high, but those skills and equipment are not used very often – such as in DR.

Now, we don’t recommend you outsource your whole DR strategy! But you should explore whether you’ll be able to afford a stronger implementation if you outsource elements of your solution to a managed service provider.

Outsourcing gives you access to a pool of DR resources and a team that maintains them, ensuring they’re available in your time of need. If an incident occurs, they’ll be able to spin up a new server, restore your data from backups, and get you back to business as usual.

A managed service provider can offer Disaster Recovery as a Service (DRaaS) at a lower price point by sharing the infrastructure (in a multitenant environment) and the team across several clients. And because the team works with many businesses, not just yours, they’ll have more experience and exposure than your in-house team would likely get.

Of course, the same applies to all outsourced IT services, not just DR. So if this is the first time you’ve considering outsourcing, you may also want to look into vendors’ connectivity, storage and compute offerings.
We’re all busy, and it can be tempting to put off contingency planning exercises in favour of more urgent tasks. But without adequate DR planning, you’re leaving your organisation vulnerable and exposed.

Don’t risk catastrophic data loss – follow the 10-step plan to keep your business operating in the face of future challenges.

Superloop is the trusted vendor of connectivity, cloud and managed services for Australian businesses, including Disaster Recovery as a Service.
Want to discuss Disaster Recovery? Get in touch!

1300 244 247
sales@superloop.com
superloop.com