15 Keys to an Effective **IT Disaster Recovery Plan**

☐

Disaster Recovery Plan

Do you have a disaster recovery plan? An effective disaster recovery plan dramatically minimises your business risk in the event of unplanned downtime. If you need help, we're here to help.

☐

Business Functions & Processes

One critical step in drafting your disaster recovery plan includes identifying mission-critical business processes, applications and documents. Have you completed this important step?

☐

Required IT Infrastructure

It's imperative to evaluate and prioritise your IT infrastructure so you can document all of your short-term critical applications, systems and networks. Have you completed this task?

☐

Supply Chain

Getting business done today often depends on third-party vendors. Have you made a list of suppliers and vendors essential to your day-to-day business operations?

☐

Risk Assessment

Building an effective recovery strategy demands understanding your unique risks. Have you identified potential natural disasters and technology-related incidents? If not, our team can help.

☐

Business Impact Assessment

Have you thought about the potential repercussions of a business disruption? Understanding probable impacts is key to developing a successful disaster recovery strategy.

☐

Financial Assessment

Determining the full financial impact of downtime for your business is instrumental in evaluating your disaster recovery plan expenses. Do you know what downtime could cost your business?

☐

Backup Strategy

Backup strategies vary, and options include on-premises, direct-to-cloud and cloud-to-cloud. Some organisations choose backup only, and others subscribe to disaster recovery as a service. Do you know which approach best suits your business?

☐

RPO

(Recovery Point Objective)

This is the maximum amount of data you can afford to lose before causing your business serious harm. This number is essential as it dictates how often you need to back up. Do you know your RPO?

☐

RTO

(Recovery Time Objective)

This is the maximum amount of downtime your business can afford. Your RTO takes into account how much time you can lose and the potential impact on your bottom line. Do you know your RTO?

☐

Insurance

With more frequent ransomware attacks and their costly payouts, many companies are turning to cybersecurity insurance. Do you have coverage? Does your insurer offer premium discounts for disaster recovery planning?

☐

Emergency Response Team (ERT)

An ERT plans for and responds to business disruptions like natural disasters and security threats. Do you have a team ready to handle worst-case scenarios like these? If not, our team can guide you through it.

☐

Disaster Recovery Team (DRT)

Your DRT is responsible for coordinating and implementing your disaster recovery plan in the event of a crisis. Do you have a DRT? If you need help deciding who from your organisation should be on this dream team, we can help.

☐

Communication & Roles

Is every member of your staff informed on your disaster recovery plan and their individual role? Does your plan include notification alerts to your emergency response team (ERT) and disaster recovery team (DRT)?

☐

Testing

Regular testing can uncover hidden gaps and keep your disaster recovery plan up to date. Do you know how often your plan is tested? Do you know how often your backups are verified? If you don't feel confident in your testing strategy, let us know.

Protect Your Data | Protect Your Business

Can you check all the boxes? If not, give us a call to schedule your complimentary assessment today.

SMIKTECK

12% of small businesses are affected by natural disasters each year.

82% of ransomware attacks target small businesses.

40% of SMBs never reopen after a disaster.

SMIKTECK PTY LTD
1300117645