NSW IT SUPPORT
Your Local IT Specialist

DELIVERING THE RIGHT BACKUP & DISASTER RECOVERY PLAN

WHEN THE CRISIS HIT YOUR BUSINESS, DOES YOUR VENDOR RESILIENCY MATCH YOUR OWN?

Back in 2011, most of the successful companies faced a significant loss of business data, where 43 per cent never reopened, 51 per cent closed its service within two years, and 6 per cent managed to survive in long-term.

Trusting your third parties is substantial and continuous to gain momentum. Organisations today are becoming increasingly comfortable migrating core and strategic functions to external providers with the objectives of accelerating growth, improving efficiency, and enabling operational transformation.

Entities take a soiled and cursory view for the recovery needs around business interruption risk. The more exposed and continually evolving functions within the organisation, the higher will be the recoverability needs. But the totality of an organisation's resiliency and recoverability needs are vaguely defined, with no mechanisms or infrastructure. As a result, the businesses lack clarity, even when moving behind the walls.

DEFINING BUSINESS CONTINUITY AND DISASTER RECOVERY

BC/DR are interchangeable despite containing overlapping elements. Business continuity planning (BCP) is a methodology used to re-create and validate plans to maintain continuous business operations before disruptive disastrous events. In the 1990s, BCP came to highlight after the businesses tried to access the likelihood of business systems failure after 2000, January 1. Since then, BCP had to work with managing the operational elements that encourage the business to function normally.

Continuous availability is indeed the subset of business continuity. Also known as a zero-downtime requirement, for some companies, it will be well worth the investment. BC/DR offers a greater tolerance for business disruption. BC/DR planning process will be different following the business nature. A small retail outlet's IT planning for BC/DR will be other from a hospital, accounting firm and government agency. There is no "one size fits all" approach fulfilling the specific needs of the company.

The objective of having a BC/DR plan is to ensure that the organisation can still accomplish its mission. At the same time, it would not lose the capability to process, retrieve and protect the information even during an interruption or disaster leading to temporary or permanent loss of computer facilities.

LEVERAGING THE DISASTER RECOVERY PLAN AND STRATEGY

Business Continuity Plan & Disaster Recoveryis designed to address issues and catalogue some of the most highly acclaimed products and services. While the Disaster recovery plans provide step-by-step procedures for recovering disrupted systems and networks, it also ascertains to assist the organisation in commencing normal operations.

The goal of these defined processes is to reduce any negative impacts on business operations. While the IT disaster recovery process identifies critical IT systems and networks; prioritises their recovery time objective (RTO); and delineates the steps needed to restart, reconfigure, and recover them. A comprehensive IT DR plan upholds all the contacts of relevant vendors, sources of expertise for reviving the disrupted systems and a logical sequence of activities and processes for a smooth recovery.

The survey report presented by National Institute for Standards and Technology (NIST)Special Publication 800-34, Contingency Planning for Information Technology Systems, the following summarises the suitable structure for an IT BC/DR plan;

- Creating the contingency planning policy statement to provide the concerned authority necessary guidance to develop a quickly executed contingency strategy.

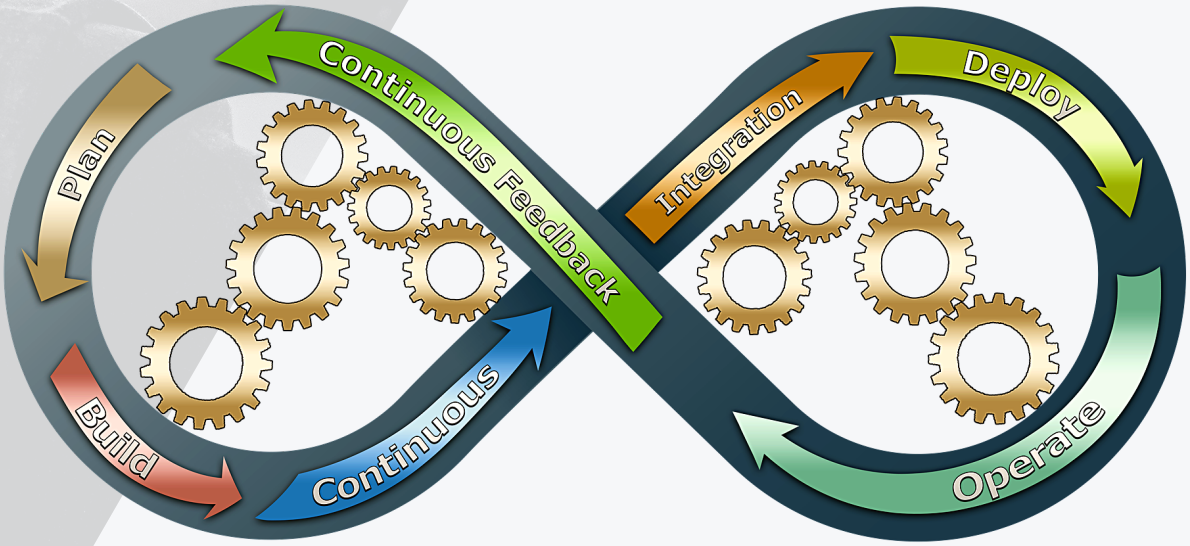
- Conduct business impact analysis (BIA) to identify and prioritise critical IT systems and components.

- Identify preventive controls. These are measures that reduce the effects of system disruptions and can increase system availability and reduce contingency life cycle costs.

- Develop an IT contingency plan containing detailed guidance and procedures for restoring a damaged system.

- Plan testing, training, and exercising of policy and strategy which identifies gaps. The training prepares recovery personnel for plan activation; both activities improve plan effectiveness and overall agency preparedness.

- The plan should be updated frequently with system enhancements.



“IF YOU DON'T PLAN, YOU PLAN TO FAIL.”

– BENJAMIN FRANKLIN

IS YOUR ORGANISATION READY TO BUILD BC/DR PLANS?

According to FEMA (Federal Emergency Management Agency), 90% of smaller companies fail within one year after a disaster if they are unable to resume operations within five days. The journey to an integrated, responsive, and proactive business continuity program walks through the business impact analysis (BIA). The BIA offers foundation and detailed view of the interruption events such as loss of facilities & technology.

"The survey shows, a 5-year-old BCDR plan is unlikely to reflect -- and prove adequate to protect -- the current IT estate."

The ideal scenario matches reality. Presently, budgets and capabilities are stretched to the breaking point, and positively charged issues such as security and regulatory compliance garner the most visibility. You may find out that your company is reluctant or unwilling to devote money or time to developing business continuity or disaster recovery planning project. The output of impact analysis includes mapping of the business process and analysis of alternative vendor. BIA identifies and evaluates the human-made and natural interruption events, vendor interruption risk assessment.

UNDERSTANDING THE DRIVERS IS THE FIRST STEP OF THE BUSINESS CONTINUITY PROGRAM.

One hour of downtime can cost small companies as much as $8,000, midsize companies up to $74,000, and large enterprises up to $700,000, according to a 2015 report from the IT Disaster Recovery Preparedness (DRP) Council. In recent years, Disaster Recovery has assumed an increasingly predominant role in enterprise computing budgets, often accounting for 20-25% of IT computing expenses.

So as a business owner are you aware of your drivers associated to the continuity program? Below are the basic insights on why you should be,

- **Recent interruptions in the industries**: Natural disasters and spark on cyber events have urged the need to develop more robust plans.
- **Focus on risk management & compliance**: Enterprises are increasingly focusing their shifts on integrated risk and compliance management to reduce compliance cost for better risk insight.
- **Reduction in downtime**: Customers demand 24/7 access to the services and products. The new technology holds high availability requirements to provide competitive customised offerings. Regulatory tolerance for critical downtime is also diminishing.
- **Third-party resilience**: Regulatory guidance now requires transparency in third-party service. The councils are also seeking insight into resiliency plans to assure portfolio integrity and fund availability.
- **Crisis managemen**t: Quick identification of external/internal response to protect and increase brand value.

THE SEVERE NOTES OF REGULATORY ON RECOVERABILITY

Regulators of every significant industry raised the bar of resiliency and recoverability capabilities. Back in October 2013, the comptrollers issued bulletin of third-party relationships, which concurrently addressed the complexity, volume, and operational interconnectedness with the third-party.

Three significant points stand out concerning third party management

- Bulletin specific considerations of the vendor resilience required as a segment of due diligence.
- Involvement of the concept of critical activities and sets of comprehensive, rigorous due diligence, management, and oversight.
- Overarching standards of the regulators implying risk-management processes involving a high level of risk and complexity.

DISASTER RECOVERY CENTER: IS THE SERVICE FLEXIBLE & RESILIENT?

If disaster strikes your organisation, where would you go? How quickly would you react? How fast can you resume your service to your clients?

Developing a business continuity plan is not exceptional but having the right technical support and experience can be of proven value. An organisation's strength depends on the ability to anticipate and respond effectively to disruptive events is key to building resilience and stake confidence.

Research from Deloitte has revealed that 90% of businesses without a disaster recovery plan fail after an event such as a natural disaster. Likewise, EMC reports, worldwide data loss and downtime cost enterprises a massive amount of $1.7 trillion (£1 trillion).

For more resiliency, flexibility and support, you can approach the service providers for,

DRC- For business continuity: The data recovery centres have premier designed facilities to protect your business data and maintain continuity of the business operations. The DRC employees the latest facilities and technology to help the affected companies resume with their operations, functions, and process.

Data suits: These are cost-effective and leading-edge solutions for businesses who wish to eliminate the expenses of establishing their own data centre facility.

Secure storage: Backing up data is one thing, and storing it safe from potential threats, and getting it recovered is the other one.

Getting peace of mind – before and after the crisis If you are looking forward to embedding BC/DR in your business, and searching for the best service provider who can take care of your business during an emergency period in Australia, contact us at support@nswits.com.au!

We add value to business!

NSW IT Support is rated 98% for client satisfaction and trust on Google Reviews! Being one of the diverse industrial clientele businesses of Sydney, we accelerate efficiency with proactiveness.

1300 138 600
info@nswits.com.au
www.nswits.com.au