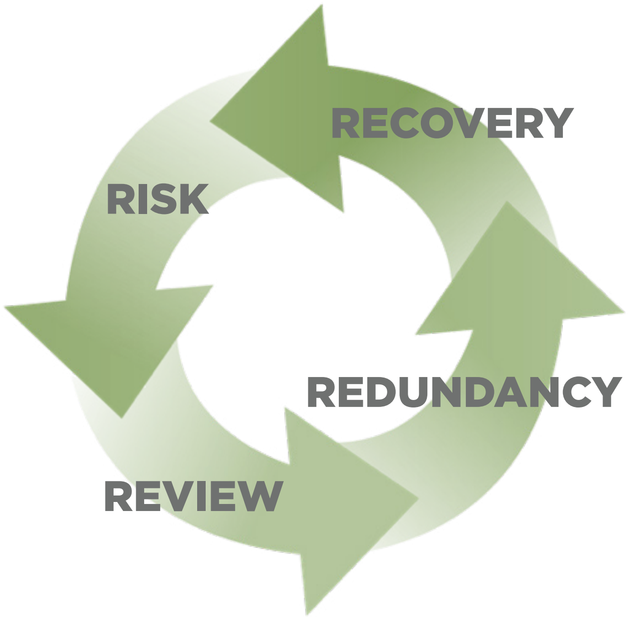
SIMPLIFYING IT DISASTER RECOVERY AND BUSINESS CONTINUITY PLANNING

Risk, Review, Redundancy and Recovery, the Four R's which are essential steps to building an IT Disaster Recovery and Business Continuity plan.



Creating an it Disaster Recovery and Business Continuity (DR/BC) plan can feel like an insurmountable task. With requirements coming from across the business, overall organizational needs, a range of budgets, and varying industry requirements thrown into the mix, disaster recovery and business continuity planning can seem daunting. Add the time and resources required to undertake the planning process and drafting a DR/BC plan ends up seeming like another set of responsibilities in addition to the demands of daily operations - leaving the IT team feeling overwhelmed.

Making DR/BC Digestible: The Four R's

In most cases, DR/BC plans can be prepared in manageable stages. Using off-the-shelf templates and IT industry best practices can facilitate the process, leading to rapid plan development and relatively easy execution.

DR/BC plans start with establishing company-wide requirements. Key stakeholders in the business must agree which IT services are essential or mission-critical, establish risk levels and potential impact to the business, and architect recovery plans based on risk tolerance. An effective approach to DR planning is following the Four R's – Risk, Review, Redundancy and Recovery – as essential steps to building an it DR/BC plan.

In this white paper, we will review the Four R's and provide supporting templates and guidelines that can be used to build the foundation of an organization's IT BC/DR plan.

The First R: Risk

RISK

A number of risks can impact the IT systems used by organizations of any size. These risks vary by geographic location, industry type, security levels and even unexpected HR threats. All IT DR/BC plans must start with assessing and understanding Risk.

A risk assessment identifies the events that could adversely affect the organization. The assessment identifies potential damage the events could cause, the amount of time required to recover and restore IT operations, and preventive measures or controls that can mitigate loss should the event occur. The risk assessment also assists with determining steps that could be implemented to reduce the severity of the event, and facilitate a rapid recovery from the event.

Risk assessments involve two forms of review: quantitative and qualitative. Quantitative risk assessment identifies the risks and measures the potential impact of risks using a numeric scale. Qualitative risk assessment identifies perceived risks by gathering information about the business using subjective terms, like "low to medium," "high or poor" "good to excellent" etc.

Using a risk assessment template and guide assists with this exercise. These templates allow IT teams and management alike to **Review** strategies that deal with the highest risks or address all risk categories. The strategies defined for addressing risk can be used to design **Redundancy** plans and plot business continuity and Disaster Recovery strategies.

The Second R: Review

REVIEW

Once the potential risks to an organization have been identified, the next step is a review of the risks. This Review, often referred to as a Business Impact Analysis, measures management's risk appetite and the organization's readiness to deal with the risks as well as determines how these risks affect specific business operations.

If all business functions are performing normally, the organization ought to be fully viable, competitive and financially solid. Should an incident (internal or external) negatively affect business operations, the organization could be compromised.

Business Impact Analysis helps business continuity/disaster recovery teams identify mission critical systems to core business functions. Using this type of analysis allows teams to consider the impact of risk on the business should certain systems become unavailable for various periods of time. The analysis will validate business requirements and lead to ranking them as part of the plan development.

A best practice is to prepare questionnaires to assist with data gathering. These questionnaires can be used as a template for on-line surveys or in-person interviews. Ideally, the questionnaire will be used to engage key personnel with in-depth knowledge and experience with the core business functions. Where possible, consider using an on-line survey to automate the process and create summaries of the data in real time.

HostedBizz

PREPARING A BUSINESS IMPACT ANALYSIS – Template and Guide

Business impact analyses help business continuity/disaster recovery teams identify mission critical systems to the business functions and analyze the impact on the business should they become unavailable for various periods of time. This will validate business requirements and lead to ranking them as part of the plan development. A best practice is to prepare questionnaires or scenarios to assist with data gathering whether by questionnaire templates or in-person interviews. Direct these questions or meetings with personnel who have in-depth knowledge of and experience with the business functions. Where possible, consider using a survey platform to automate the process survey with the results being captured and summarized in real time.

When formulating the questions, include realistic scenarios that describe potential incidents for interviewees to assist them with answering questions. Examples could include situations such as:

- All records, data files, technology and other support systems are lost;
- Access to critical IT systems is lost due to a cyber-security attack
- Certain key IT personnel are suddenly available;
- An essential business unit's (e.g.: finance) portion of the building is completely destroyed;
- Primary business processes or applications will be affected immediately and for at least 30 days;
- A IT disaster occurs during a peak business period for the business unit.

Incident descriptions help frame the interviewee's response so it can be in alignment with specific risks and threats.

Ultimately, the BIA's purpose is to identify, prioritize and document the relative importance of various business processes conducted by business units.

When formulating the questions, include realistic scenarios that describe potential incidents to assist respondents with answering questions.

Examples could include situations such as:

- All records, data files, technology and other support systems are lost.
- Access to critical IT systems is lost due to a cyber-security attack.
- Certain key IT personnel are suddenly unavailable.
- An essential business unit's (e.g. finance) portion of the building is completely destroyed.
- Primary business processes or applications will be affected immediately and for at least 30 days.
- An IT disaster occurs during a peak business period for the business unit.

The BIA identifies, prioritizes and documents the relative importance of various business processes conducted by business units. A link to a BIS Template is shown below.

Link to Business Impact Analysis Worksheet

The Third R: Redundancy

REDUNDANCY

When it comes to IT, redundancy can mean many things. In its most simplistic form, redundancy refers to the backup of the business data stored on servers, network attached storage, or desktops. In the broader sense, redundancy can be applied across several IT sub-systems including, server hardware and storage, network hardware & access, power, backup systems and even secondary work sites. The level of redundancy required for each of these systems is derived from the Review (Business Impact Analysis).

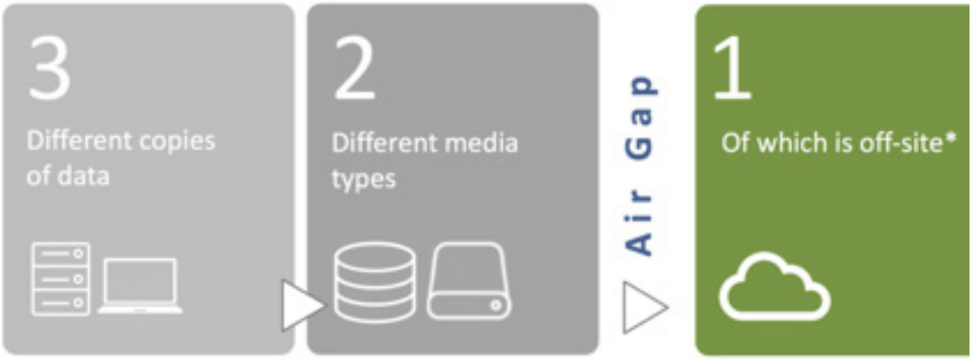
Factors that should be considered and will influence decisions around IT redundancy include:

- Compliance and Security requirements for the industry that the business operates in.
- Criticality of the services that the business provides.
- Consequences to the business in the event of IT outages.
- Budget.

The level of importance that is assigned to each of the factors above determines the extent of redundancy that is implemented with each IT system.

Regardless, a best practice is always to ensure that three (3) copies of data are always available: one in production; a second stored as a local backup copy; and a third stored as a copy off-site – preferably with a cloud backup service provider. This creates an "air gap" between on-premise systems connected to the local area network and the offsite backup to ensure data is safe and unaffected by the risks identified in the first phase of the DR plan.

Three copies of your data : The 3.2.1 Rule



Budget is often the factor that influences the selection of hardware deployed by the business. However, even if budget is not a factor, having all IT systems (redundant or otherwise) in a single location may not be best for the business. Consider ranking critical systems by importance to the business and using defined backup levels (file level, image-based, and full replication) based on the criticality and restore time requirements. Finally, using a qualified Disaster Recovery as a Service (DRaaS) Provider can help address all of the Redundancy and Recovery requirements for a business.

The Fourth R: Recovery

RECOVERY

The final and most critical step of the IT DR/BC plan is the Recovery capability. The effectiveness of the plan is ensured through continuous recovery testing. In continuous testing, the primary objective is to identify deficiencies with the DR/BC plan and to ensure the data integrity of the recovery. Selecting the most secure backup provider will allow for recovery tests to be done in isolation from production systems including recovery tests from offsite backup copies to the cloud using cloud servers. Ideally, successful tests result in full IT system recovery without incident. However, tests that appear to be "successful" and uncover no problems should also be suspect. Uncovering and documenting recovery problems present opportunities to fix problems before a disaster happens.

Key strategies for testing include starting simple – perhaps with simple file restores and eventually full server and applications recoveries. Increasing the difficulty of the test involving vendors and other stakeholders, or even launching surprise tests, will help reveal the effectiveness of the disaster plan and recovery capabilities.

When launching a testing exercise program, start with a plan review and outline of the expected outcomes. This will help with managing the test recovery and assist with staff being comfortable with the testing process. As the tests improve, increase the level of test complexity. Remember that if a test "fails" it is not a failure. Rather; it is a success. It is far better to identify systems and procedures that may fail, and rectify them, before a real incident occurs. Finally, a true test is to launch a surprise incident. This will truly test how well prepared the company and the IT systems are to address a real incident.

The Truth of DR/BC Planning

The Four R's make DR/BC planning manageable and easy. By using the provided template, an organization can engage stakeholders, gather company-wide requirements, establish essential business services and acceptable risk levels, and design recovery plans based on risk tolerance. The four R's – Risk, Review, Redundancy and Recovery – help to organize DR/BC planning and provide focus along the way.

Selecting a hosting provider needn't be a burden on your organization.

For more information about how HostedBizz can help establish your DR/BC plan, visit our website: www.hostedbizz.com.

About HostedBizz

HostedBizz is a leading Canadian IaaS and Cloud Service Provider. We offer an integrated suite of cloud services that help businesses transition their on-premise IT systems to a fully managed, enterprise-grade cloud computing infrastructure. Our goal is to leverage the operational benefits of the cloud while helping businesses to reduce business risk and costs.

To learn more about the HostedBizz cloud infrastructure or to work with our professional support team, visit www.hostedbizz.com

BUSINESS IS BETTER IN THE CLOUD.
OUR CUSTOMERS ENTHUSIASTICALLY AGREE.

Discover our enterprise grade cloud services for business without the enterprise cost