**Disaster Recovery Outline**

**Lucas Rodholm**

**5/5/2024**

Contents

[Project Concept and Executive Sponsorship 4](#_Toc181640468)

[DR/BC Introduction 5](#_Toc181640469)

[DR/BC Risk Assessment 6](#_Toc181640470)

[Safeguarding Critical Assets 7](#_Toc181640471)

[Storage and Communications 9](#_Toc181640472)

[Off-Site Backups 9](#_Toc181640473)

[Cloud Computing 10](#_Toc181640474)

[Unified Communications 11](#_Toc181640475)

[Voice Communications 11](#_Toc181640476)

[DR/BC Plan Implementation 12](#_Toc181640477)

[Mitigation Plans 12](#_Toc181640478)

[Policies and Procedures of the DRP 13](#_Toc181640479)

[Who is Responsible for Writing Procedures? 14](#_Toc181640480)

[Approvals 14](#_Toc181640481)

[Training 15](#_Toc181640482)

[Emergency Response Team (ERT) 16](#_Toc181640483)

[Testing and Maintenance 17](#_Toc181640484)

[Testing Example 17](#_Toc181640485)

[Maintenance 18](#_Toc181640486)

[Audits 18](#_Toc181640487)

[References 19](#_Toc181640488)

# Project Concept and Executive Sponsorship

This document will reflect a conceptual outline of a disaster recovery/business continuity (DR/BC) strategy for the fictional organization ‘ABC Marketing Solutions.’ This is an organization of roughly 1,000 employees who use their industry knowledge and work as a team to implement, support, and maintain marketing strategies for organizations of all sizes.

Having an effective DR/BC plan for ABC Marketing Solutions is a top priority. In the event of natural disasters, physical damage to business assets/information, cyber-attacks, or any other incidents which stop business production, ABC Marketing Solutions is at risk of losing stakeholder interest, clientele, credibility, and revenue without the implementation of an effective DR/BC plan. It is important for businesses or organizations of all sizes to finalize a DR/BC strategy so that downtime can be minimized, and assets/data may be safely recovered.

Executives in ABC Marketing Solutions’ corporate office have relayed instructions to ensure that data is one hundred percent recoverable and may be *securely* retrieved during a disaster. Clients of ABCMS include organizations with sensitive data such as billing information, addresses, names, marketing strategies, and more, which makes securing this information in an offsite location very important. To clearly understand the magnitude and significance of a DR/BC plan, corporate executives have requested a formal business impact analysis (BIA), communication response plans, scheduled testing, and maintenance strategies.

With these instructions provided, andthe overlying importance of a disaster recovery plan, executive sponsorship is necessary for progressing the project, acquiring adequate funding, and helping to develop a solution which aligns with the company policies and vision.

# DR/BC Introduction

With the oversight of an executive sponsor, the creation of a disaster recovery and business continuity plan is initiated. Hiring or delegating employees to manage the disaster recovery plan is the first step. These positions include:

Executive Management: Just like the examples above about executive sponsorship, this position oversees the project and maintains alignment with company goals and policies.

Crisis Management Coordinator: The crisis management coordinator will initiate the plan and communicate with various team members and departments. This position emphasizes the flow, coordination, and progression of the plan and all recovery efforts.

Business Continuity Expert: The business continuity expert will align the vision and goals of the company with recovery efforts and provide clear communication of these goals to the recovery and IT team. This role serves as a bridge between executives and technical team members.

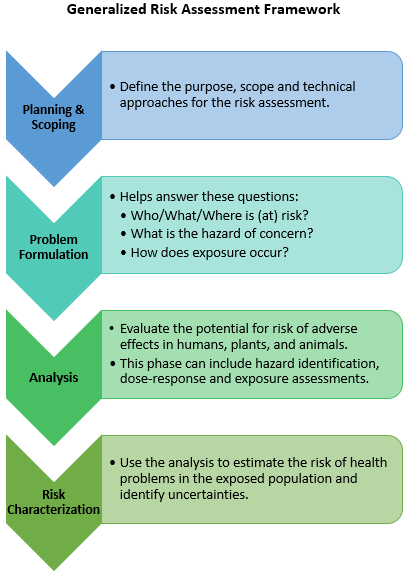
Impact Assessment and Recovery Team: Collectively, the impact assessment and recovery teams should be knowledgeable of the network, storage, server, and database infrastructures *and* be able to execute recovery methods in these fields.

(*Disaster Recovery Team & Who Should Be Included | Flexential*, 2017)

Further implications of the DR/BC plan include budgeting, insurance coverages, physical resources, personnel, network infrastructure, data management systems, compliance policies/requirements, and risk assessments. (Brush & Crocetti, 2022)

# DR/BC Risk Assessment

Developiung and utilizing risk assessments will help the organiztion to make decisions based on a myriad of risks and their overall impact on business conituity. In some instances, a risk assessment may help determine if a risk is tolerable *or* if it will cause disruption and discontinuity which may be considered *intolerable*. These assessments help to identify hazards early on and create plans for dealing with them if/when they present themselves.



# Safeguarding Critical Assets

Just like many other organizations, ABC Marketing Solutions requires databases systems for a multitude of data to be stored, such as employee information, client documentation, contracts, billing, addresses, application software, login information, and much more. These items are critical to protect and must be accessible so that business operations may continue in the event of a disaster. It is important to maintain security and accountability of these assets so that the organization does not forfeit credibility due to data loss or cyber attacks.

Asside from digital assets, disaster recovery also relies on safeguarding physical assets from damage, wear and tear, natural disasters, or lack of maintenance. This includes servers, workstations, network infrastructure, or anything that is used to perfrom business operations. These investments are the tools which drive the company and must be properly managed and accounted for in a disaster recovery or business continuity plan, *to* *include* proper budgeting. It is important to review risk assessments and budget accordingly so that the organization is prepared to fund maintenance efforts, regular updates, and replacements if necessary.

A diagram of a cloud company

Description automatically generated

Protecting and backing up these critical digital assets illustrates the importance of cloud computing, where data is backed up routinely and retreived easily during disaster recovery. Cloud solutions are scalable, secure, and highly available, providing high levels of support and customization. Utilizing a cloud computing service to store and recover critical data eliminates single points of failure because the cloud service is completely separate from the local network. Creating a redundant network environment is detrimental to preserving operations and minimizing downtime. This includes the use of failover systems at critical failpoints, or areas of the network where fault tolerance and high availability are imperative. Whether that is a phone communication system, router, storage drive, software application, etc., the failed node can pass responsibility to the backup node(s) and continue operations as if nothing ever happened.

Using risk assessments, impact analyses, and device lifecycle charts help the organization to prepare for future costs and maintenance efforts. This itemization of costs is then packaged for DR coordinators and business continutiy experts to present to executives and to the DR team. Maintaining critical assets requires the delployment of a well trained team which regularly monitors the network, updates software, firmware, and hardware devices, and routinely tests systems for vulnerabilities and functionality. These are significant measures which aid in disaster recovery efforts and benefit the organization.

# Storage and Communications

### Off-Site Backups

A main consideration when developing a disaster recovery plan for an organization is backup storage locations that can be utilized in the event of a cyber-attack, natural disaster, or any other form of data loss from a central storage location. Three major types of disaster recovery sites are as follows:

**Cold Sites**

* Advantages
  + Provides power and networking capabilities to ensure network availability and uptime.
* Disadvantages
  + Requires installation of backup data and hardware before becoming fully functional.
  + Cold sites do not offer storage capabilities

**Warm Sites**

* Advantages
  + Provides all capabilities of cold sites, such as network availability, while also including storage devices and hardware, such as servers, drives, etc.
* Disadvantages
  + Data is required to be regularly transported to the warm site with no automation capabilities. This maintenance requires resource expenditure.

**Hot Sites**

* Advantages
  + Obtains all cold and warm site capabilities as well as automated data mirroring, making this the best option for disaster prevention and preparedness.
* Disadvantages
  + All of these capabilities require resources and upfront hardware/software investments.

### Cloud Computing

Cloud computing back-up capabilities offer their own list of advantages and disadvantages, too. They are beneficial to organizations of all sizes for back-ups to off-site locations in case recovery efforts are needed. Cloud services are offered and charged to the client based on elements such as capacity, bandwidth, number of users and data egress. (Crocetti, 2023) A cloud computing disadvantage that stands out is the simple fact that cloud service providers are outsourced and standards such as security, accessibility, and recovery time are out of your control. All in all, the cloud storage option is very appealing for companies that need a reliable backup location while able to tolerate the risks.

### Unified Communications

Unified communication is extremely important to an organization’s disaster recovery/business continuity efforts. This form of communication connects the organization to a single communication platform which is beneficial to distributed architectures such as remote offices and multiple locations. UC also guarantees information to come from a verified, internal source. With these considerations, it is important that ABC Marketing Solutions adopts and implements a trusted unified communication system. (*Learn How Unified Communication Aids Business Continuity*, n.d.)

### Voice Communications

ABC Marketing Solutions currently relies on a phone system that is locally operated with no redirecting or cloud capabilities. This single point of failure violates the disaster recovery plan and should be mitigated by contracting a cloud-based phone solution provider to set up call-forwarding and system functionality from a cloud location - even when local equiptment fails. Having reliable voice communication helps control disaster recovery and response efforts and improve business continuity statistics. (Bryan, 2019)

.

# DR/BC Plan Implementation

### Mitigation Plans

**Prior to an Event**

To minimize losses *before* a disaster event takes place, there are a few important items that must be implemented in ABC Marketing Solutions’ DR/BC plan. First, a risk assessment which covers all possible disasters and disruptions to business continuity should be clearly defined. This includes all possible hazards, natural disasters, vulnerabilities, human error, and additionally creating an impact analysis to determine the criticality of these risks. The impact analysis should include all possible repercussions including financial and operational impact.

Once a detailed risk assessment is established, it is important to implement a strategy for preventing and reducing these risks. The risk assessment and impact analysis should clearly outline a strategy so that the only thing left is implementing the required components. This includes backup power supplies (UPS devices and backup generators), a physical security system (locks on doors, key access, personal ID cards), proper employee training procedures, redundant infrastructure wherever possible/necessary, off-site backup locations, up-to-date hardware/software, and more. As stated above, this list should be extremely detailed with *clear* direction provided by the risk assessment, impact analysis, and availability requirements. With all of these details ironed out and documented, it is important to perform regular testing and constantly communicate test results to executive management as well as the DR/BC team.

**During an Event**

While any organization would love to only test and simulate their disaster recovery plan, the unfortunate truth is that one day it will need to be utilized, and more importantly, it will need to perform. The type of disaster does influence the response of the DR/BC plan; however, the steps required to continue business operations, recover data losses, and restore the business are well-defined in the plan and should be followed. After all, this plan is developed with the help of executive management, stakeholders, and professionals on the DR team, so the next step is *execution*.

**After an Event**

At the conclusion of an event, it is important to test operational abilities and ensure that the plan was effective in mitigating the disaster and continuing business operations. Once these tests are verified, documentation and audits are saved and reviewed by the DR team and those involved in the recovery process. There is some light in a disaster recovery event which includes the ability to learn from the experience and adjust the DR/BC plan accordingly. If there’s one thing that is certain, it’s that a DR/BC plan is never set in stone. They are ever-evolving and require constant care, maintenance, and testing.

### Policies and Procedures of the DRP

Step one of recovery is to open lines of communication (utilizing UC) to connect the organization to a single communication platform. The next step is to assess the damage and coordinate recovery efforts based on this discovery. It is beneficial to refer to the impact analysis and risk assessment to assist with decision making and mitigation strategies.

For many organizations, including ABC Marketing Solutions, it is extremely important for business continuity to be prioritized so that during the event, services can still be provided to clients. For data center recovery, this means quickly recovering data from off-site (hot site) locations and providing the organization with the means to access data and continue normal operations. In the event of a network failure, it is important to utilize redundant infrastructure and failover techniques to keep the network afloat. Lastly, in the event of a human-caused or natural disaster, it is important to ensure that all critical equipment or software fails over to off-site cloud locations and is replaced or repaired as soon as possible. (*What Is Disaster Recovery? - Features and Best Practices*, 2024)

### Who is Responsible for Writing Procedures?

Specific procedures that must be included in the DR/BC plan will often change depending on many factors, such as company growth, changes to infrastructure, budget, etc., but these procedures should always be documented and collaboratively outlined between the DR team, executive management, and stakeholders.

### Approvals

Approval is required to instill these policies and procedures and must be provided by executive management and stakeholders. After all, the DR/BC team may be more knowledgeable about *how* to execute the plan than executives, but they are not able to create any procedures unless a contract is approved to provide adequate funding to the team.

### Training

* + **Executive**

At the executive level, members should be trained in the importance of disaster recovery and business continuity. They should be in-tune with risk assessments and impact analyses so that they are well-informed and able to make critical decisions that the organization relies on.

* + **DR/BC team**

The DR/BC team will require constant training to ensure that all necessary precautions are taken to prevent disasters. If an incident occurs, they should be trained on their individual duties and given all required information to allow them to perform their duties at a high level. For instance, the IT team should have extensive knowledge and documentation about the current infrastructure, assets, devices, software, and so on.

* + **Middle managers**

Middle managers have very important roles to connect upper management to DR/BC teams, meaning they should be trained to easily bridge this communication gap. This includes extensive knowledge of the team’s duties as well as how they pertain to upper management and the decisions that need to be made.

* + **Department heads**

Just as middle managers must bridge communication between teams and executives, department heads must act as a liaison between middle managers and individual departments of the DR/BC team.

* + **Employees**

Employees should not only be trained in how to perform their required recovery duties, but also in how to prevent user/human errors. Although the turnover rate of employees may be higher than other positions (management), it is important to quickly train them in the importance and criticality of their roles and responsibilities.

* + **Suppliers**

Suppliers are often forgotten about in DR/BC training efforts; however, ensuring that suppliers are aware of recovery methods and continuing the use of supplier services is very important to business continuity.

### Emergency Response Team (ERT)

The emergency response team at ABC Marketing Solutions should involve the entire DR/BC team, including employees, department heads, middle managers, and executive management. The ERT is triggered by a disaster where each team member or team plays a critical role:

1. DR/BC team assesses risk and impact, presenting this information to department heads.
2. Department heads will oversee these efforts and communicate their findings to middle managers.
3. Middle managers will communicate with executive managers to request guidance (approval).
4. Executive managers will take all the information given to them to make a decision and provide approval to the middle managers.
5. Middle managers will communicate the approval and additional information (if applicable) to the department heads.
6. Department heads and DR/BC teams will work together to mitigate the disaster and quickly restore operations.

# Testing and Maintenance

### Testing Example

During a scheduled test of the DR/BC plan, systems were reported to be taken offline and not properly restored. Additionally, databases were corrupted, and all communications have been lost. This is a complete failure of the plan; however, according to Ton (2017), there is no such thing as a DR/BC test *failure*. The point of these tests is to learn, adjust, and further develop the plan until a successful restoration is achieved.

In order to avoid the failure situation that occurred, there are a few adjustments that need to be made immediately. As stated earlier in this document, utilizing unified communications (UC) to establish a platform in which the organization (specifically those involved in DR/BC) may communicate internally is of upmost importance. In the failed test, communication was completely lost, which drastically decreases the likelihood of a successful restoration. This derives the need for a fully operational UC platform and *unit testing* procedures to ensure that internal and external communication is operational.

The DR/BC test yielded beneficial information about failures to restore systems and recover data from data centers. Avoiding system-restoration failures involves *reviewing* the individual systems that failed to operate after testing and *reevaluating* the ways in which these systems are backed up. The same applies for data recovery, ensuring that data is continuously backed up to a highly available cloud server and recovered within RTO specifications.

Once a disaster event has ended and all systems/data has been restored, the team must thoroughly document the entire event, what went wrong, and how it was resolved, including metrics which are measurable and comparable to initial DRP expectations. As stated above, it is important to learn from the test and constantly evolve so that these failures recur in the future.

### Maintenance

Maintaining a disaster recovery plan entails annual reviewing and updating significant changes to system architecture, system dependencies, or recovery personnel. Additionally, regular testing on individual components of the DRP as well as simulations of abrupt and unscheduled losses of critical functions are *required* efforts for ABC Marketing Solutions to include in their maintenance plan. (*Maintain Your Disaster Recovery Plan / safecomputing.umich.edu*, n.d.) Between constant reviews, testing, and checking backup locations for functionality, a DR/BC plan will evolve into an invaluable asset to the organization and its success.

### Audits

With the right approach, auditors add value to the organization and executive management by ensuring that the DRP provides effective coverage and protection when a significant disaster occurs (Swanson, 2022). Audits should be conducted annually, or whenever significant change occurs, such as the examples above. The purpose of auditing is to ensure that the DRP is up-to-date and compliant with organizational needs, goals, and regulations.

# References

* *Disaster Recovery Team & Who Should be Included | Flexential*. (2017, December 6). Flexential. <https://www.flexential.com/resources/blog/what-disaster-recovery-team-and-who-should-be-included>
* Brush, K., & Crocetti, P. (2022, May 18). *disaster recovery plan (DRP)*. Disaster Recovery. <https://www.techtarget.com/searchdisasterrecovery/definition/disaster-recovery-plan>
* Technologies, I. (2012, November 30). Types of Disaster Recovery Sites: Cold, Warm, and Hot Sites. *iCorps*. <https://blog.icorps.com/bid/101789/types-of-disaster-recovery-sites>
* Crocetti, P. (2023, January 19). *Cloud backup vs. traditional backup: Advantages, disadvantages*. Data Backup. <https://www.techtarget.com/searchdatabackup/feature/Cloud-backup-vs-local-traditional-backup-advantages-disadvantages>
* *Learn how unified communication aids business continuity*. (n.d.). <https://www.essentialtech.com.au/blog/how-unified-communications-aids-business-continuity>
* Bryan. (2019, December 29). *How can I create a disaster recovery plan for Voice?* McEnroe Voice. <https://mcenroevoice.com/can-create-disaster-recovery-plan-voice/>
* Zivaro. (2022, January 25). 10 Simple Ways to Disaster-Proof your Business Today | ZIVARO. *Zivaro*. <https://zivaro.com/disaster-proof-your-business/>
* *What is disaster recovery? - features and best practices*. (2024, April 2). Cloudian. <https://cloudian.com/guides/disaster-recovery/disaster-recovery-5-key-features-and-building-your-dr-plan/>
* Resolver. (2023, September 15). *Metrics That Matter In Business Continuity & Disaster Recovery | Resolver Resources*. Resolver. <https://www.resolver.com/resource/bcdr-metrics-that-matter/>
* Ton, J. (2017, September 1). There is no such thing as a DR test failure. *CSO Online*. https://www.csoonline.com/article/562785/there-is-no-such-thing-as-a-dr-test-failure.html
* *Maintain your disaster Recovery plan / safecomputing.umich.edu*. (n.d.). https://safecomputing.umich.edu/protect-the-u/protect-your-unit/disaster-recovery-management/maintain#:~:text=Disaster%20recovery%20plans%20must%20be,systems%20hardware%2C%20and%20so%20on.
* Swanson, D. (2022, September 21). *Auditing Your BCP and DR program – Just How Resilient is Your Organization?* Risk and Resilience Hub. https://www.riskandresiliencehub.com/auditing-your-bcp-and-dr-program-just-how-resilient-is-your-organization/#:~:text=Audit%20tests%20in%20reviewing%20a,%2Dto%2Ddate%20(e.g.