QUICK START GUIDE

# Quick Start Guide to Business Continuity and Data Recovery

Powered by

IT Security
COMMUNITY

CompTIA.

Data is the lifeblood of the modern enterprise. Today’s businesses store and mine vast amounts of electronic information on products, processes, customers, sales, and more. Google collects enough data, if printed and stacked on top of each other would reach the moon in just two days. The mission-critical information ecosystem businesses now rely on to survive and thrive include: Mobile devices, Electronic Medical Records, Internet of Things (IoT), cloud applications and services, virtualized environments and big data repositories.

# Business Continuity and Data Recovery 101

Our goal with this Quick Start Guide is to help you, as a solution provider, to develop internal Business Continuity and Data Recovery procedures, documentation, and exercises that will support you company's goals. What you learn while developing these for your organization will prepare you to build real world solutions for your customers.

Let's unwrap some of the jargon to prepare you for this journey:

"Business Continuity" and "Data Recovery" are not interchangeable terms. In fact, as a solutions provider, you can build very successful practices for each. These terms act as two distinctly different but interconnected parts of risk management.

**Business continuity** is a comprehensive proactive plan focused on long term operational issues of the business. The plan identifies the people, processes and technology required to continue operations in the event of a Business Interruption. For manufacturers, the plan needs to ensure operations continue when when upstream or downstream providers are unable to deliver goods to manufacture the product or even ship the final product. For a medical practice the plan would include how to bill, contact patients, and conduct business. When developing a BCP, it is important to identify the critical, nice to haves, and wants of the business.

**Disaster Recovery Plan**, for the point of the Quick Start Guide, includes step by step recovery plans for applications, vendor contact information, and recovery prioritization of the system that support the business. Initiation of the plan typically starts with a loss of access to data no matter the cause.

**Risk Assessment**, is the systematic process of studying the areas of potential risk to corporate operations. With the advent of cloud computing, conducting a risk assessment can have a significant number of 3rd parties whose risk must be identified.

**Data Replication**, is the method to make copies of data for use in the event of a data loss event. Typically, the data is replicated locally then copied to a remote system or service.

**Redundancy**, is creating multiple paths to the same set of systems. Redundancy does not have to only include networking, servers, and disk storage. In certain situations, a business during their business continuity planning exercises will identify secondary vendors who can provide services if the primary vendor is unable to deliver.

**Fail Over**, is the process to switch over from the primary equipment to the secondary equipment. In the event of an outage, having a fail over plan with supporting redundant systems allow mission-critical systems and process to continue with little or no disruption.

**CIA**, Confidentiality, Integrity, and Access are foundational measurements when building a BC or DR plan. A good plan will identify how to successfully recover from, or continue business operations for each component of the CIA triad.

**Crisis Communication Plan**, is meant to coordinate communication to staff (where to report to work, etc.), and an external communication plan (what to tell partners, customers, etc.). A key component of the plan is to identify the roles that can communicate status to employees and who is the spokesperson for the public.

# Background

The harsh truth is while organizations grow increasingly dependent on electronic assets, many have ignored the basic safeguards of proper business continuity and data recovery. Many technology solutions provider have not implemented the essentials of BC/DR. The cost of such disregard can be staggering. When disaster strikes, network operations are disrupted and the business could grind to a halt without a plan. As a parent, have you even been at the amusement park with hungry kids? However, the line for the food the kids want is 20 people deep? A parenting continuity plan is to have a baggy of snacks. Hand the snacks out to the kids and the "I am hungry" meltdown is avoided.

Businesses impacted by an outage suffer long-lasting damage to their brands, reputations and even open themselves up to litigation. The grimmest report is from Gartner which states that a business that has a catastrophic data event has a two year survival rate of just 6%. As important, CDW research indicates that 82 percent of significant network disruptions in U.S. businesses could be reduced or avoided by implementing even the most rudimentary data recovery and business continuity processes.

Given the ubiquity of fast internet connections and cost effective cloud based data storage, there is no real reason not to have a BC/DR plan in place. In their "The State of Enterprise Risk Management 2016" report, Forrester Research shows that 49% of the respondents indicated that the cost of an unprepared BC/DR response forced the organization to reprioritize strategic investments. The 2016 study by Markets and Markets expects the spend on DR as a Service (DraaS) to grow from $1.68 Billion dollars in revenue to $11.11 Billion by 2020. The market is growing rapidly and to support this growth well-trained solution providers are needed.

# BC/DR Planning Life Cycle

As a solution provider, you've likely had a hand in developing the systems that generate, process, communicate, and store much of your customers' burgeoning business data. No matter how carefully architected, implemented, and maintained, those systems will eventually fail. However, businesses that you support cannot typically afford to fix everything all at once. Prioritization of the systems critical to key business process is essential in reaching the customers' business continuity goals.

As the trusted advisor, the solution provider will have deep knowledge of customers' business operations. The more you know about your customers the more you can help them. Clients in manufacturing and retail will need continuity and recovery plans that focus on customer and partner access and supply chain integrity. Others in highly regulated spaces such as finance, health care, or government will require focus on data recovery aspects such as data confidentiality, integrity, and availability for example.

Here is a simple process to go through to develop the necessary and comprehensive plans:

**1. Start with the policies and standards from the organizations risk management policies.**

a. These policies will anchor the rest of the project

b. Policies will guide decisions such as acceptable risk, where staff will show up, any associated compliance requirements

c. Technical Standards will identify the available server/software options the organization currently has

**2. Develop the business continuity plan.**

a. Document the business process and how they are supported by people process and technology

b. Identify and communicate with stake holders and SMEs

c. Build consensus on continuity and recovery priority, and recovery time objectives

**3. Then develop the disaster recovery plan.**

a. Based on Recovery Time Objectives build solutions to meet the needs

b. Develop step by step recovery documentation for current state. Modify as required as changes occur

**4. Implement the necessary changes to support the goals of the plan.**

a. Develop options for the customer

b. Select solution and create a Build of Materials

c. Implement the solution and update documentation

**5. Test the plans.**

a. At an agreed upon time, test the recovery plans

b. Keep track of any changes needed for the plans

c. Confirm with customer that the goals are met

**6. Maintain the plans**

a. Over time, system software upgrades and network changes will change and could enable new options

b. Keep documentation current

Process for Developing BC/DR Plans for Customers

- Start with existing policies and standards of their risk management. Use them to anchor the decisions of priority.
- Leverage this Quick Start Guide to assist in the specific planning.
- Develop continuity plans based on the level of priority.
- Develop disaster recovery plans based on the level of priority.
- Manage process changes required to support the plan.
- Test the plan's effectiveness with mock run-throughs.
- Maintain and update the plans over time.

When promoting the BC/DR offerings of your organization, it is important to share that contingency plans must be in place to effectively mitigate these risks. No matter which business vertical you work with, keep in mind the major categories of risks that businesses face

1. **Environmental** – Heat, cooling, server or network gear failure, or power failure, bankruptcy, etc.
2. **Vendor** – Failure by vendors, software, communication outage, non-performance to support SLAs, etc.
3. **Natural** – Earthquake, flooding, tornado, fire, etc.
4. **Human** – key employees leaving the organization, human error (intentional or unintentional), opening infected email attachments

# Planning

The end-game of the advance professional service work by the solution provider is the development and delivery of a business impact assessment (BIA). A BIA requires a thorough understanding of not just vital business processes, but also the interdependencies and relationships among the client's people, processes, technology, and services.

BIAs should map continuity and recovery priorities including lines of jurisdiction, areas of primary business concern, and the order systems will be restored in the event of disruptions. BIA serves as the best tool for continuing the discussion on business continuity and recovery needs with the customer and for selling long- term BC/DR support and management engagements.

When starting out the planning process, have a minimum checklist of the following:

- Roles and responsibilities
- Resource availability (Money, Personnel, and Time)
- Business recovery objectives
- Project communication plan
- How has the client reacted to previous outages or data loss?
- Any other necessary deliverables

A significant part of the BIA will come from determining the customer's data loss tolerance. While some data loss is inevitable in any organization, determining the amount and what types of data a business can lose without a detrimental impact to the business is crucial.

Work with the identified employees with the responsibilities to identify:

1. **The system, its business function, and who supports it**
2. **Is the application on a supported release?**
3. **Is there a current support contract with the vendor?**
4. **When was the last time testing of the backup process occurred?**
5. **What are the upstream and downstream applications and business processes affected by an outage of this system**
6. **Recovery Time Objective**
7. **How well is the customer technologically positioned to take advantage of a modern BC/DR offering?**

There will be many ways to track and provide documentation based on the information that is collected during the interviews. One method is to have a spreadsheet that across the top has at a minimum the following columns (A more complete example is available online).

| Application (Version) | Owner | Supported version | Upstream systems | Downstream systems | Business process impacted | Backup schedule | Last test of backup | Recovery objective | CIA Score |
|---|---|---|---|---|---|---|---|---|---|

Once the grid is completed, develop a graphical representation of the interconnectedness of the business processes, systems supporting those processes, staff supporting those processes, and IT assets. During the first review with the customer many application owners will be jockeying for position as having the most critical system that must be recovered. Having a document that demonstrates the connection points will provide the visual cues so that the customer's management is able to clearly identify the key components, processes, or personnel. Not all systems can be priority #1. During a disaster, staff from both the business and the IT team can only work on recovering only a single system or process at a time.

Take the feedback from the meeting and spend time refining the Business Impact documentation. The systems that support the business will typically be stratified into three tiers based on their business impact score.

1. **Tier 1** – systems are the highest priority and include those IT assets that would put the business at risk with even the briefest outage.

2. **Tier 2** – system outages are ones business can tolerate. They can last a few hours or up to several days before the organization is impacted.

3. **Tier 3**– systems can be down for longer periods and are generally noticeable only to IT.

As the backup and recovery specialists, you should be prepared to quantify each category with supportable uptime and availability metrics so they can be incorporated in the Service Level Agreements.

# Disaster Recovery Design

When designing recovery options for your customer, keep in mind a study conducted in the UK shows that 24% of all data loss is caused by human error, 21% from hardware failure, and 19% from data corruption. That is a whopping 64%.

As stated before, recovery cannot happen all at once. Utilizing outdated or unreliable technologies will not support the recovery objectives. Take time to work with the client to balance the cost of recovery. The pre-DR phase is the appropriate time to optimize hardware, networking, storage, security, applications and bandwidth. All of which are a significant upselling opportunity even before the BC/DR service is sold.

There are many methods to balance the cost of recovery. In the past, most systems had to be recovered on identical equipment. Virtualization can help you deliver cost effective continuity and disaster recovery solutions. It is during this phase of the project that you will determine which of the customer's servers will serve distinct roles and how many physical versus virtual copies are needed to assure solid BC/DR footing.

This complete DR plan is a step-by-step document detailing the necessary recovery steps and technical specifications. It includes elements such as:

- who is responsible for declaring a disruptive event and mitigating its effects;
- scheduled recovery exercises;
- how the customer will communicate with the solution provider;
- where client employees are expected to do their jobs and how they will be contacted.

While BC/DR is often seen as strictly a technology issue, a truly effective strategy needs to blend people, process and technology in a coordinated effort to keep the customer's business operational under most conditions.

# Choosing A Delivery Model

Solution providers have several options for delivering and supporting business continuity and data recovery services. The choice of a BC/DR delivery model will depend on the solution provider's expertise and resources, and the unique vertical needs of the client. Choices include:

## TRADITIONAL MANAGED SERVICES

After the assessment phase, the solution provider implements a co-located infrastructure and associated BC/DR tools and provides ongoing maintenance, monitoring, and support of the system. The solution provider is contractually obligated to deliver agreed- upon systems availability per an SLA and will coordinate data and network recovery in the event of a disruption. Managed service providers already accustomed to remote monitoring and management, as well as business operations automation and 24X7 support should excel in the managed BC/DR services role.

- **Advantages:** Includes a broad mix of both transactional sales and recurring-revenue services. Customized services can be delivered.

- **Disadvantages:** Initial investment costs for co-located equipment and equipping recovery "cold sites" are higher than other models. Level of solution provider BC/DR expertise required is high.

## CLOUD-BASED MANAGED SERVICES

Includes many of the aspects of the traditional managed services relationship, but leverages third-party Software and Infrastructure-as-a-Service offerings to support BC/ DR elements including data replication, network and connectivity redundancy, and applications availability.

- **Advantages:** Recurring revenue opportunity. Lower cost of entry and less staff technical BC/DR expertise required.

- **Disadvantages:** Limited ancillary hardware/software sales and smaller overall profit margin. Limited ability to customize for customers in specific verticals. Less solution provider control of user data can complicate SLAs.

## PROFESSIONAL SERVICES

Involves the assessment phase, crafting both the BIA and the comprehensive BC/DR plan, coordinating recovery practice exercises, varying degrees of involvement with system architecture, solutions recommendations and implementation.

- **Advantages:** Low barrier to entry for solutions consultancies and other service providers with limited access to data center infrastructure or skilled BC/DR IT staff. Gives solution providers an alternative option to work with clients under strict regulatory constraints or committed to internal control of BC/DR systems.

- **Disadvantages:** Less opportunity to develop recurring revenue sales or leverage relationship for related infrastructure transactions.

Regardless of the model chosen, solution providers must evaluate their sales and marketing capabilities to determine their ability to profitably deliver services like business continuity and data recovery which are highly customized, multi-discipline and heavily weighted toward consultancy. Standardized pricing models rarely fit in such consultative relationships; solution providers should build and price proposals in a way that considers protracted deployments and long-term delivery of services, advice, and continuously updated expertise in BC/DR technologies and best practices.

# Seven Steps to an Optimum BC/DR Offering

With assessments done, SLAs in place and delivery model chose, the solution provider must now frame the business continuity and data recovery discussion into a real-world offering that dependably protects the customer's business.

### 1. Create Resilient Data Protection

Ensuring the client's Tier 1 data is protected and demonstratively recoverable begins immediately. That usually means backing up to a remote, off-site data center that is properly certified and far from the customer's home offices. Low-cost options like tape backup might seem attractive but can significantly delay recovery due to the slow recovery speed of tape. In addition, if you need to restore to the last full backup and then sift through incremental backups to find the data in question, you can quickly find yourself out of compliance with SLAs. And if any incremental backups failed, the data could be lost forever. Cloud based and disk-to-disk backup and recovery have become extremely cost effective and the technologies of choice because of their flexibility and reliability. The bottom line: make certain the backup schema is compatible with your customer contract and conduct ongoing tests to validate effectiveness.

### 2. Ensure Real-Time Application Backup

Most backup vendor tools support standard files and databases, but they vary widely in their ability to handle files that are open and in use. In practice, the data that is most needed during recovery is data that was in use during backup, so this functionality is key. The ability to handle a variety of operating systems and applications that require specialized backup support (Microsoft Exchange, Microsoft SQL Server, VMware, for example) is also vital for crafting a system that delivers in the real world.

### 3. Create a Compliance Checklist

Many companies and their data are subject to the rigors of regulatory compliance. Whether they fall under the common rules of Payment Card Industry Data Security Standards (PCI-DSS) or are required to meet the strict provisions of specialized regulations such as the Health Insurance Portability and Accountability Act (HIPPA), the Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley (SOX) or the Dodd-Frank Wall Street Reform and Consumer Protection Act, the solution provider must ensure that BC/DR systems and any related partners or vendors conform to these industry- specific requirements. For optimum protection, it is generally best to choose solutions that encrypt data during transmission and storage and move backups to an offsite data center that is appropriately certified (SOC 1 or 2). The customer should also be the only one who has the recovery key.

### 4. Consider the Cloud

A 2016 report by CloudBerry Lab found that 49% of businesses have a single copy of their data. 36% of businesses do not have a full copy of their data. There is huge market potential for data recovery and business continuity to utilize SMB Cloud based DRaaS. Planning with the Cloud in mind can be greatly simplified with judicious use of available cloud computing technologies. Just make sure that the customer is not surprised by the expenses. Some have described the use of Cloud services as a Death by a thousand cuts (meaning tons of one off charges for network bandwidth, CPU, and disk). Current cloud-based solutions provide the necessary underpinnings for such data recovery mitigation assets with greatly reduced implementation time and cost.

### 5. Don't Ignore Mobile Devices

The explosion in workplace mobility is driving new business continuity and data recovery needs unheard of just a few years ago. Today, more than 70% of employees in the US carry some sort of company-owned mobile device. The Ponemon Institute recently found 62% of lost or stolen mobile devices contained sensitive corporate data while just 39% of businesses have any sort of security in place to mitigate that risk. This, coupled with an increasing number of BYOD initiatives allowing employee-owned devices to access corporate data, means incorporating mobility into the BC/DR strategy is a must for any solution provider. Utilize application virtualization to allow the utilization of company applications without exposing the data to additional loss or security risk. In addition, talk with the customer about providing a data backup solution for all of the data on those laptops. Recovering a damaged drive in a laptop can cost thousands of dollars. Losing the data can cause extreme hardship on the organization as well.

### 6. Future-proof Your Solutions

The initial assessment likely already describes the basic tools you'll use to manage your customer's systems. But considerations remain for actual solution choices and implementations. For example, the customer may indicate a desire to bring data management back in- house as the company grows. Choosing a solution at the outset that would facilitate such a move seamlessly is vital to the long-term success of the project. Flexible solutions let both you and your customer decide how exactly to implement BC/DR for optimum success.

### 7. Don't Forget DR for Cloud Data

Some cloud vendors come and go. The needs of your customers might outgrow the capabilities of the initial cloud service provider. It is critical to treat a cloud provider who hosts corporate data the same as you would treat the data recovery of on premise systems. This includes negotiating data backups, SLAs for network and system connectivity, and securing the data within the hosted application and hosted data center. A regional hosted hospital data exchange in Illinois recently shutdown with no notice. It took a court order to force the company to continue operations while the data was pulled out of their systems.

### Recovery Options for Virtual Systems

When selecting virtualization for disaster recovery and business continuity, there are different options for backing those systems up. Though there are many options when backing up a Virtual Machine, there are typically two options that work the best. Image level backups is one option in using backup software/appliance that will backup the VM Image. Remember that a VM is simply a large file that is changed at the block level, just like a document. To reduce the time and size of the backup, a second option is available called block level incremental backups. This methodology allows a full image backup initially, then any block level changes. This also allows for data deduplication as well. There are systems that now enable a recovery of a VM in under 5 minutes. Simply amazing when compared to tape.

# Future Opportunities

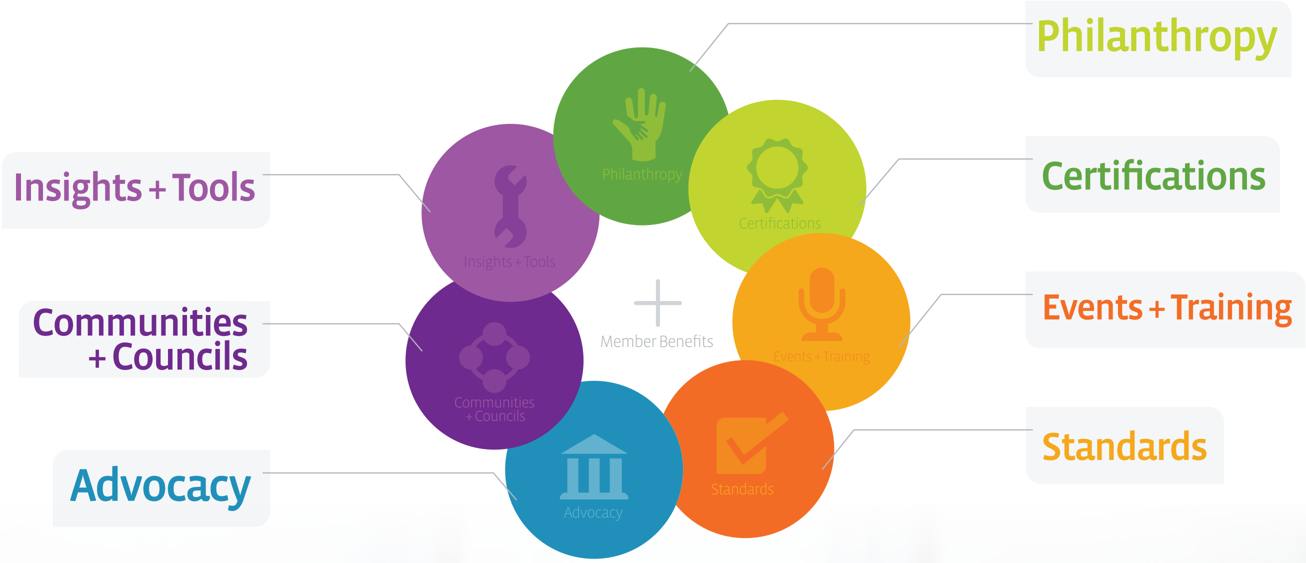
Optimizing existing business continuity and data recovery deals means evolving the relationship beyond the basics and helping customers turn fundamental BC/ DR systems into long-term business strategies. Solution providers that master the continuity and recovery offering of today can develop the enhanced systems of tomorrow by continually reviewing the client's changing business needs and data requirements to wring out ongoing opportunities in storage, networking, security and applications. Sales that began as largely consultative arrangements designed to map out BC/ DR strategies can become profitable recurring-revenue relationships that mix high-touch professional and specialized managed DR services with transactional sales and natural extensions into related business and technology services.

One area of opportunity for BC/DR solution providers is the expansion of virtualized systems, and particularly virtual desktop infrastructure (VDI), as a driver for enhanced continuity and recovery capabilities and efficiencies in a growing enterprise. Many clients will outgrow basic BC/DR protections as their organizations enlarge to include more data, data sources and repositories, and physical geographic locations. The ability to quickly distribute updated server and desktop images that virtualization and VDI affords, for example, can turn a basic BC/DR arrangement into a lucrative next-generation project engagement. Solution providers specializing in networking and infrastructure are best positioned to promote advanced server virtualization and VDI solutions to leverage such cutting-edge technologies to improve continuity and recovery strategies that protect the business and reduce long-term costs.

Similarly, advanced cloud and mobility services can piggyback on the BC/DR relationship for enhanced services delivery from the solution provider. Another next-step opportunity exists in the burgeoning business intelligence and analytics space. Solution providers with hands-on knowledge and experience with their customers' data ecosystems are uniquely positioned to assess the potential for advanced analytics to drive business innovation and growth for their clients. These high-touch, high margin relationships give end users new or enhanced abilities to view, combine and analyze diverse data sets resulting in radically new insights into their business processes, sales and marketing initiatives. The result is a business that operates more efficiently with an enhanced competitive advantage.

The challenge for solution providers then is to be willing and able to continually assess the existing business continuity and data recovery environment with the goal of developing more comprehensive business strategies that take full advantage of the access, insight and structural awareness these modern data-protection technologies afford.

CompTIA. Creating the Keys to Technology's Future



Philanthropy

Certifications

Events + Training

Standards

Insights + Tools

Communities + Councils

Advocacy

**Who We Are**

CompTIA is a Global Tech Trade Association and the Voice of the Industry

**Our Mission**

Advance the Tech Industry

**Our Members**

Tech Solution Providers, Vendors, Distributors and Consultants

Coming Soon-Tech Professionals, Educators and Students

Join Today

CompTIA.org/register

CompTIA

Powered by

IT Security
COMMUNITY

CompTIA.org