FADDOM

The Quick-Start Guide to BCDR Successs

And How Application Dependency Mapping Can Support Your BCDR Goals

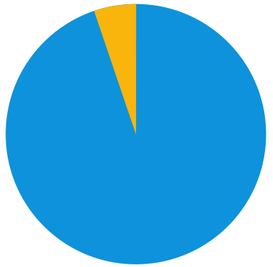
It takes years to build up a successful business. But it can be destroyed in almost an instant.

A potentially catastrophic event can wreak havoc on an organization at any time—**from a power outage, extreme weather, and hardware failure to an internal or external cyberattack or accidental deletion of mission-critical data.**

That's why smart companies put business continuity and disaster recovery (BCDR) measures in place. So, if the worst should happen, they can keep going and get back to normal operation with the minimum of disruption.

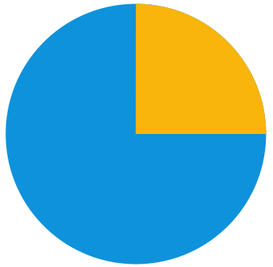
However, the task of developing a robust BCDR plan can be daunting for virtually any organization of any size.

That's where this guide can help. It takes you through the key points you should consider as part of your BCDR strategy and also discusses how application dependency mapping (ADM) can support your BCDR goals.



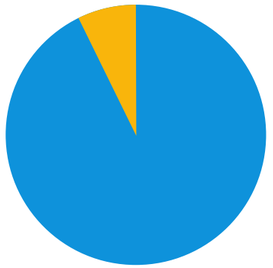
96%

of organizations had experienced at least one outage to their IT infrastructure in the past 3 years – LogicMonitor



25%

of businesses fail to reopen following a disaster – US Federal Emergency Management Agency (FEMA)



93%

of companies that suffer a major data disaster without having contingency measures in place go out of business within a year – phoenixNAP

FADDOM

What Is BCDR?

BCDR is a series of closely related **business continuity** and **disaster recovery** practices that focus on how your organization should respond to an adverse and highly disruptive event.

Business continuity deals with the issue of how to keep your organization operational throughout the period of disruption. In terms of your IT, it includes:

- a failover system you can call upon if your primary infrastructure goes down
- remote working arrangements

Disaster recovery, on the other hand, is the set of provisions you make for restoring your systems to normal operation as quickly and efficiently as possible. It includes:

- a regular backup routine
- a mechanism for restoring your systems from those backups

Business continuity and disaster recovery are complementary to one another, but neither is specifically designed to prevent a disaster. Nevertheless, they're an important part of your data protection strategy, as they help minimize the impact to your business in the event of an emergency.

What Is ADM?

ADM solutions are a class of IT asset discovery and monitoring software designed to gather information about your application dependencies and present it in a way you can easily understand it.

They provide this information in two different forms—a **spreadsheet**, listing details about the different services your application uses and the connections between them, and a **visual map** of your application ecosystem. This visual representation makes it easy to see the interactions and relationships between the different components of your applications, helping you to understand how they work together and affect one another.

ADM tools also continually monitor your applications so you always have up-to-date insights into your deployments.

ADM Use Cases

As we'll discover later, ADM can play a key role in your BCDR strategy. But it's also useful in many other use cases, including:

- IT Documentation
- IT Asset Management (Change Management)
- Data Center Transformation
- Cloud Migration Planning
- Microsegmentation
- Network Security Operations

What Are Application Dependencies?

Dependencies are the ecosystem of components an application relies upon so it can function as intended. They include:

- Servers and subnets
- The underlying operating system
- Files and database systems
- Libraries and frameworks
- Proprietary software
- Other in-house codebases

BCDR Planning and Implementation

If your business is relatively small then your BCDR initiative may only necessitate a few basic measures. But if you're a large-scale enterprise, with complex IT deployments, you'll need a much more detailed **response plan** and a far more sophisticated BCDR implementation.

The following are the main considerations you'll need to take into account.

Roles and Responsibilities

People will be just as important as your technology for getting your business back on its feet as quickly as possible. So, as part of the planning process, you'll need to appoint members of staff to your BCDR team and designate roles and responsibilities accordingly.

This should involve people with different skills, knowledge, and job roles to ensure all aspects of BCDR are fully covered—from system and recovery requirements to the ongoing task of testing, reviewing, and updating the BCDR plan.

Furthermore, a diverse team will help ensure everyone understands their role in the event of a crisis and can enter into action with a quick and well-coordinated response.

Communications

During any extended period of disruption, you'll be under intense pressure to get business operations back to normal just as soon as you can. So you'll need to keep your workforce fully informed and manage expectations.

ADM will give you visibility into your applications so you know whom to contact during a crisis. For example:

- development, operations, and database administration teams
- users of the software and those of any applications that integrate with it
- customers and suppliers who are affected

In addition, your plan will need to include provisions for external communications, such as who will be responsible for liaising with enforcement authorities and the media.

Emergency Working Arrangements

With the recent trend towards remote working, organizations are now far better adapted to a sudden switch to emergency working arrangements.

But not every company is able to manage without an on-premises workforce. In such cases, a BCDR plan should give due regard to contingency measures such as emergency office space, a standby generator, and other infrastructure and equipment to keep your operation moving.

And don't forget that remote working presents challenges to cybersecurity, as employees can easily put your systems at risk through careless working practices. So make sure you have appropriate policies in place to prevent security shortcomings such as misconfigured personal devices and unencrypted home Wi-Fi networks.

Backup System

Even if you have a regular backup testing regime, a restore still might not work when you actually need it. Not only that but your backups are also at risk of attack by malicious actors.

So you should never just rely on a single backup copy of your data.

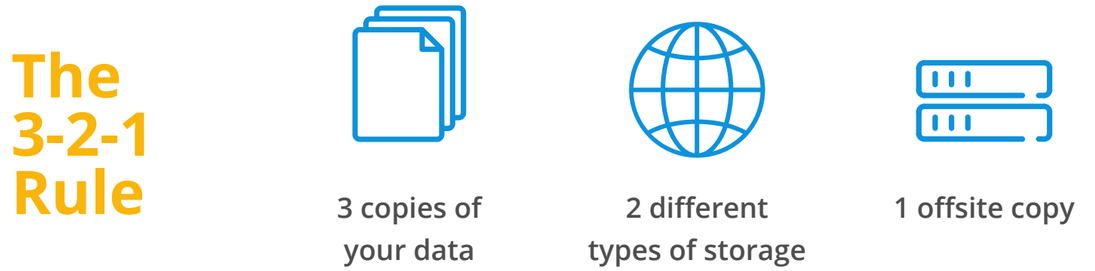
One way to ensure adequate protection is to follow the **3-2-1 backup rule**. This is a rule of thumb in which you maintain at least three copies of your data. In an on-premises setting this would be two local copies, your production data and a backup on a different storage medium, and another copy in a separate location such as the public cloud.

The local backup provides you with a readily accessible copy that should be quick and easy to restore. However, it's more likely to be affected if a disaster directly impacts your on-premises site.

The offsite backup, on the other hand, is at much less risk of being affected by the same disaster. Furthermore, it will be effectively air-gapped from your on-premises data center, making it more difficult for adversaries to perform a successful **ransomware attack**.

However, for complete protection, at least one of your copies should be an **immutable backup**, which doesn't allow anyone, even users with admin privileges, to modify, encrypt, or delete data until the end of a predetermined retention period.

Immutable backup technology is available both for on-premises storage devices and as cloud-based solutions.



Failover System

A failover system is an alternative method of replicating your data, which you may need to consider as part of your 3-2-1 backup strategy.

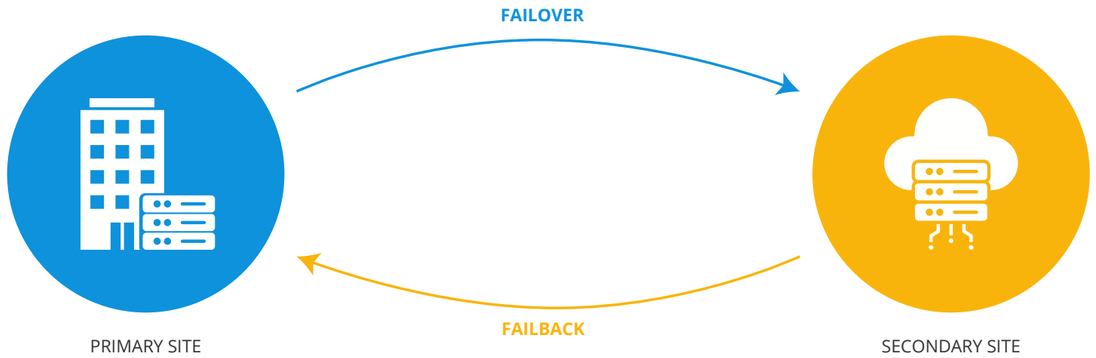
It is a business continuity mechanism in which you can seamlessly switch to a secondary standby environment in the event your primary system goes down. It also provides failback functionality, which allows you to switch back to your primary site once it's back up and running.

The public cloud is a particularly good fit for a failover system. This is because you need only provision enough resources to keep it running in the background. You then only need to scale up capacity when you need it in an emergency.

The main problem with failover systems is that they're notoriously complex to design and build. However, ADM tools make the task significantly easier by giving you the visibility you need into all your application components. This will help

ensure you take the entire functionality of an application into account and, as a result, help reduce potential dependency issues that can lead to crashes or issues with data consistency.

Backup and failover complement one another. But it's important to be aware that failover isn't a substitute for backups. This is because it cannot protect you in certain circumstances. For example, corrupted or infected files will replicate across your primary and secondary sites. And, unlike backups, you cannot use failover to recover from any malicious or accidental deletion of data, as this will also synchronize between live and standby environments.



Recovery Objectives

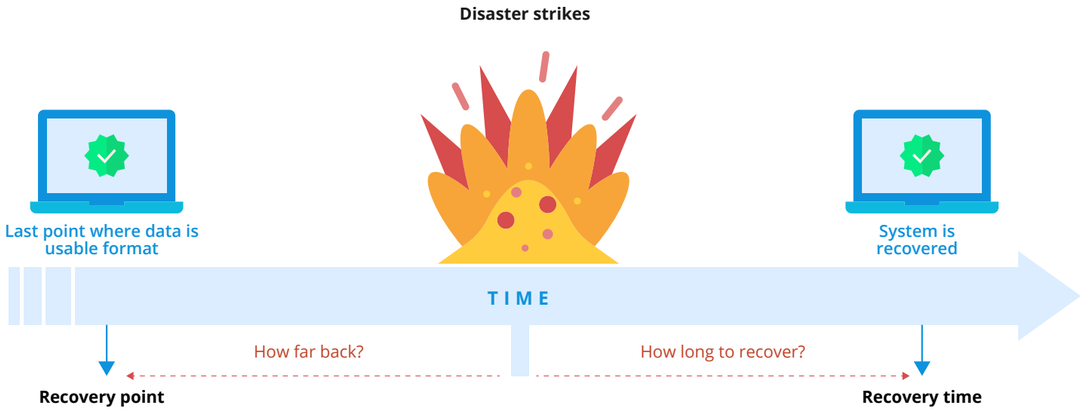
Your BCDR plan should include a **recovery time objective (RTO)** and **recovery point objective (RPO)** for each of your backups.

RTO represents the period of downtime your business is prepared to tolerate following a disaster. In other words, how long it can acceptably wait for a system to resume normal operation.

RPO is also a measure of time and represents how far back you're prepared to roll back without an unacceptable loss in up-to-date data. It determines how often you should schedule your backups, as dictated by the amount of data loss your business can tolerate in the event of a disaster.

For example, it's important to set a low RPO for a system that processes financial transactions. By contrast, you'd be able to accept a far higher RPO for a dev/test environment, which doesn't store mission-critical data.

In general, the more frequently you take backups and the faster you need to restore them, the higher the cost. You'll therefore need to weigh these costs up against requisite recovery timeframes of the business.



Recovery Checklist

You'll need to consider the order in which to restore your systems to ensure the recovery process runs smoothly and the disruption has minimum impact to your business overall.

Mission-critical applications will be of top priority, along with **internal email servers** so staff can communicate with customers and each other as soon as possible.

Bear in mind that many business applications share the same data and are tightly integrated with one another. So your recovery checklist will need to take dependencies into account to prevent errors, access issues, and system crashes as you bring your systems back online. For example, you'll need to restore **authentication services** as early as possible, as users won't be able to access other applications until you do so.

ADM tools can have an important hand in setting such priorities by showing you the relationship between your applications and their dependencies, including the data flow between them.

And don't forget company politics when setting recovery priorities.

ADM can also help by showing stakeholders across the business how each of their applications forms part of a wider picture. This can help overcome objections from users of applications that are lower down in your list.

Compliance

Finally, you should be mindful of regulatory compliance if you host backups or a failover system in the public cloud. This is on account of data residency and data retention obligations under data protection laws such as the **General Data Protection Regulation (GDPR)**.

For example, in common with many other similar regulations, you may only process and store personal data in those countries permitted by the GDPR.

This applies to the data not only in your production environment but also in your backup systems. So, if you host a backup or failover mechanism in the cloud, you need to make sure the cloud regions you use comply with such requirements.

> **Some data, such as personally identifiable information or some financial data, is regulated no matter if it sits on a production server, a backup server, or even on magnetic tape.**
>
> — David Linthicum, best-selling author and internationally recognized cloud computing expert

BCDR Maintenance and Testing

Your organization is forever changing.

Employees move in and out of job roles. You adopt new technologies in a bid to drive your business forward. You continually roll out software patches and updates. And you replace infrastructure as it reaches the end of its useful lifetime.

As a result, your BCDR preparations can quickly go out of date. This can have severe consequences if they no longer work as intended just at the moment you call upon them.

That's why regular maintenance and testing is so important to your BCDR endeavors. So make sure you include the following in your list of ongoing commitments.

Backup System

Your backups have the potential to get corrupted just as with any other data.

Incremental backups can be particularly vulnerable, as they're usually constructed from a chain of preceding incremental snapshots. This means that if one snapshot becomes corrupted then it doesn't just become unusable but so do all subsequent recovery points later in the chain.

So don't neglect to periodically test your backups. From time to time, you may need to start again from scratch by taking a new full backup before continuing with further incremental snapshots.

Also be aware that scheduling systems can fail to trigger your backup jobs. And that the backup process can fail altogether.

So, above all else, make sure you regularly check you are actually taking backups.

Backup Hygiene

If you need to recover data following a cyberattack, you may discover your backups have also been infected.

So make sure you regularly scan them for malware. This complements existing security measures and mitigates the impact of a breach by ensuring they're clean and safe for use in a system restore.

Failover System

The complexity of failover systems not only means they're a challenge to implement but also to test and maintain. In most cases, this involves system downtime that can impact the productivity of your business.

But, again, it's important to remember that your IT environment is always changing. So you simply cannot afford to set it and forget it then expect it to work seamlessly when you need it.

ADM can, at least, help you overcome much of the complexity of failover testing and maintenance. It continually monitors your applications for changes and tracks the movement of data between different application components. As a result, you'll always have an up-to-date picture of your application topology so you can adapt your mirror system to any changes accordingly.

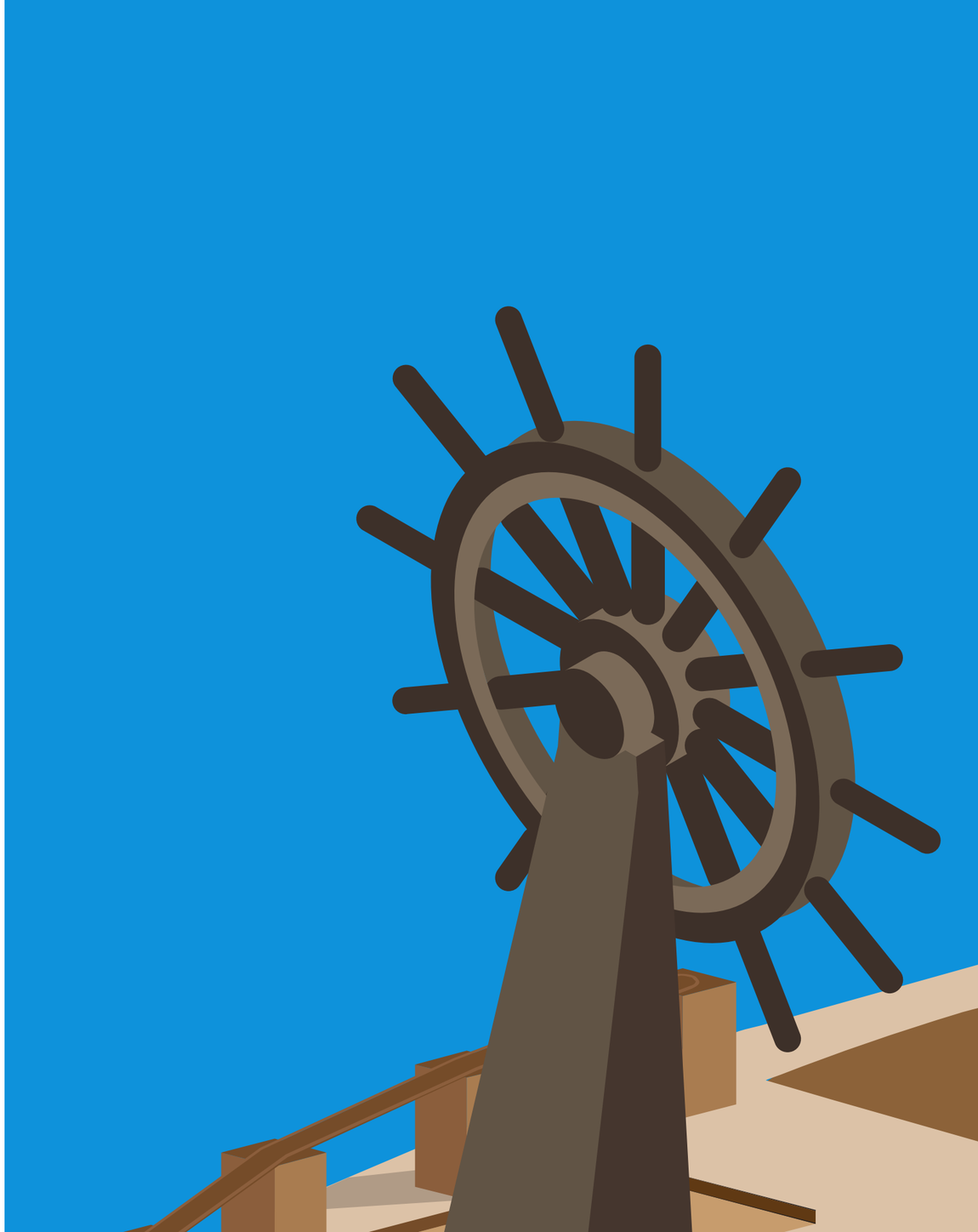
And be aware that failover testing should go beyond simply checking whether your standby system works. For example, you'll need to make sure your secondary infrastructure can cope with the real-life resource demands placed upon it. Furthermore, you'll need to test your failback process works as expected

The Whole BCDR Plan

You shouldn't just test your technology but your entire BCDR strategy. That way, everyone in your business will know how to respond in a real-life situation.

It will help you monitor the performance of your BCDR team. It will help you identify weaknesses in your plan and iron out unexpected issues. It will help you test whether you can meet agreed recovery timescales.

But, above all, it will help ensure you're fully prepared for any disaster that comes your way and avoid potential consequences that could even bring your company down.



About Faddom

Faddom creates interactive, real-time maps of your entire IT ecosystem, offering granular detail. Our solution is completely platform-agnostic and has limitless use-cases. Uniquely, Faddom works without credentials, firewalls, or agents. With network discovery based on real traffic, you gain ultimate visibility of all dependencies and communications. Use this to efficiently assess costs, discover a hybrid ecosystem, or model workloads for migration.

Our platform is easy to deploy, highly scalable, and can be integrated with all of your current tools and products seamlessly. Whether you are primarily on the cloud, utilize hybrid or multi-cloud environments, or reside on-premises, Faddom can

be used to discover, plan, and maintain the most comprehensive real-time map for your application ecosystems. You can easily configure your map to manage IT assets by business context, prioritizing the right alerts and, more importantly, keeping your business running smoothly.

Contact us at
info@Faddom.com
to see a live demo.