RESTECH SOLUTIONS

BCDR FOR BUSINESS:

THE 7-STEP PATH TO CONDUCTING A BUSINESS IMPACT ANALYSIS (BIA)

Proactively Understand How Outages Can Impact Your Organization

Contents

Introduction

All businesses, irrespective of their size, industry or location, are prone to disruption. This could be anything from temporary loss of service due to poor internet connectivity, to severe downtime caused by a storm or a breach. The key to not getting overwhelmed by disruptions is to prepare in advance. Trying to counter the effects after they have occurred is often far more costly. After all, prevention is better than a cure.

Drawing up a comprehensive and effective risk management strategy is critical to combating disruptions of any sort. One of the main components of an effective Business Continuity and Disaster Recovery (BCDR) strategy is a **Business Impact Analysis (BIA)**. A BIA can help you ramp up your business' security, compliance and backup postures and go a long way towards ensuring your business runs smoothly.

What Is a Business Impact Analysis?

Regardless of whether an accident, storm or full-blown cyberattack disrupts your business, you need to determine:

- How it will affect your business
- Which resources should be prioritized
- What approaches you need to take to recover quickly and minimize losses

This is where a BIA comes in by helping you:

1

Identify critical business functions.

Identifying vital functions lets you create a business continuity and disaster recovery (BCDR) strategy powered by robust security, relevant compliance and reliable backup.

2

Quantify the impact of disruption on the above functions.

You can express the impact in terms of cost to the business.

BIA for BCDR

A BCDR strategy outlines the necessary steps you must take to bounce back quickly following a disruption.

A BIA lays the foundation for a robust BCDR strategy and prepares your business for potential or inevitable disruption.

In short, BIA coupled with BCDR enables your business to reduce downtime and ensure productivity even during times of crisis. We will discuss more about this a little further along.

BIA Components

Three key components make up an effective BIA. These are business impact, timeframes and dependencies.

Business Impact

As specified earlier, a BIA identifies a business' most essential functions. It includes identifying vital business processes, crucial resources within these processes and critical systems involved. Once complete, the expenses associated with disruption, such as drop in revenue, regulatory penalties and hike in operational costs are calculated in monetary terms for each business function.

A more practical approach considers the non-monetary effects of disruption as well, such as loss of reputation.

You can start conducting a BIA with a simple questionnaire that contains questions such as:

- What would the financial impact be if a particular business function goes down?
- How much in fines or penalties would regulators impose on you?
- By how much would the operating cost increase?
- What would be the effects on the business' reputation?
- What conditions would trigger a process outage?
- What is the probability of the recurrence of the risk?

Timeframes

Your business should address three main timeframes:

1. Recovery Point Objective (RPO)

RPO is usually measured in seconds and represents the amount of work that can be lost in the event of a disruption. Loss of work beyond this limit can cause significant damage to the business.

2. Recovery Time Objective (RTO)

RTO is usually measured in minutes and represents the time it takes before employees can start working after a disruption event.

3. Maximum Allowable Downtime (MAD)

MAD represents the duration after a disruption event beyond which the impact caused by zero/minimal output becomes severe.

Dependencies

A BIA can be used to determine the dependencies of business processes and systems. It lets you prioritize the resources that need quick recovery and helps you understand the order in which functions or processes need to be restored. Always prioritize operational business functions—apps and services—over less critical functions like testing.

It is also possible—and likely—to have vendor dependencies amongst mission-critical functions. This includes IT vendors, ISPs, etc., and you'll want to document them in your BIA.

Additional Resources

The following standards could act as a guide on how to create a BIA:

- The Federal Financial Institutions Examination Council's BCP standard for financial institutions
- International Organization for Standardization's standard 22301

Executive Sponsorship and Commitment

An effective BCDR strategy begins with sponsorship and commitment at the highest levels of the organization (owners/stakeholders/board members and senior management). A BIA framework with sponsorship has an endorsement from a top-level executive who will oversee and help it progress.

In the absence of executive sponsorship, conducting a BIA might not be as effective and threats could seep in through the cracks unchecked.

Steps to Secure Executive Sponsorship

Although getting executive sponsorship is not easy, its significance in the successful implementation of a BIA makes it worth securing.

1. Identify a suitable sponsor

A good sponsor can oversee, support and ensure better resource/fund allocation to a BIA. Asking the following questions can help you identify a suitable sponsor:

- **Will the sponsor be by your side when the going gets tough?**

  Conducting a BIA and using the results to upgrade the business' counter-disruption strategy is a big lift. It is not just a one-time process. Regular review and updates will be needed. You may encounter multiple hurdles along the way, and you need to know that the sponsor is committed to long-term success.

- **Can the sponsor understand the effort you are putting in?**

  The right sponsor can sync with you quickly and understand the amount of effort you invest in addition to providing excellent suggestions and advice.

- **How does the sponsorship improve the executive's standing within the organization?**

  Find a sponsor whose department can benefit from having access to and give inputs on a BIA. Ideally, this will be a mutually beneficial situation and not just a one-way investment.

- **Does the sponsor sufficiently understand BIA?**

  The sponsor must have an adequate understanding of what a BIA entails and must be able to comprehend the information you provide.

- **Why did the sponsor back certain programs and not others?**

  This will give you a better understanding of the sponsor and their competencies/interests as well as availability to support your BIA initiative.

2. Prepare a business case

Prepare a business case outlining how the compliance program will benefit the business and the executive. Consider it your sales pitch. Keep it brief, comprehensive and capable of evoking interest in the potential sponsor. Explain how taking on this additional responsibility will improve outcomes related to their specific realm of influence or enhance their standing within the organization. Conveying benefits through numbers is advisable, especially if you are trying to communicate:

- **How many employees would suffer due to a disruption**
- **How much revenue would be lost following a disruption**
- **How a BIA can help improve productivity and protect revenue streams**

3. Schedule a meeting

Scheduling a meeting with a top executive can be challenging because they usually run on tight schedules. So, the key to arranging a meeting is to be professional, assertive and concise. If the executive you are trying to schedule a meeting with has an assistant, contact them first to explain what you are trying to accomplish and seek their input about how best to approach the request.

- **Let the potential sponsor know the time required for the meeting.**
- **Convey the benefits of conducting a regular BIA.**
- **Remember to mention your expectations from the sponsor.**

4. Request executive sponsorship

Present your business case in such a way that all intended information is clearly communicated to the executive. Make sure the presentation is engaging and syncs with the interests of the executive. Here are a few tips to help you succeed at this stage:

- **Never exceed the time limit.**
- **Set aside some time for questions and feedback.**
- **Start with an overview of what a BIA is and what it does.**
- **Explain the multitude of problems that a BIA can solve.**
- **Introduce the team that will be handling BIA matters.**
- **Specify how you intend to make the BIA framework successful in the long run.**
- **Mention all the benefits of a regular BIA in monetary terms.**
- **If your first choice declines the proposal, ask them to recommend another.**

BCDR: Beyond Backup

Although business continuity and disaster recovery (BCDR) is a concept that has been around for over 20 years, it can still be confusing. In an era where any loss of data can result in severe complications for companies, it's critical that every business understands BCDR in depth.

The pandemic ushered in a new set of challenges, with businesses now dealing with distributed workforces, accelerated adoption of the cloud and an increase in ransomware attacks. You can no longer depend on an outdated BCDR strategy that relies on backups alone to address these issues.

Always remember that your work is not complete if you simply draft a BCDR strategy and leave it untouched. Not reviewing and testing your BCDR plan regularly could prove to be a critical mistake since IT systems and processes are changing at an unprecedented pace.

To make BCDR part of your business' resiliency roadmap, you must update it frequently and think beyond just backups. **A comprehensive BCDR strategy incorporates elements of security and compliance as well.** Experts estimate that the frequency of ransomware attacks will increase every year.[1] With such alarming numbers causing panic, many companies have changed their perception about BCDR. Have you?

A comprehensive BCDR strategy:

Protects Critical Systems and Processes

Once the BIA determines which systems and processes are vital to the business, you must ensure your BCDR strategy covers them through a combination of effective and robust backup, security and compliance tools.

Ensures the Integrity of Sensitive Data Assets

The complexity of today's work environments — that includes scattered locations like the cloud, on-premise and remote locations — affects the integrity of data assets. That is why it is crucial to deploy:

- Security tools to protect data
- Compliance solutions to ensure data handling as per regulations
- Backup solutions to protect your business against data loss

Fuels the Business Resilience Roadmap

A comprehensive BCDR strategy not only prioritizes and ensures business continuity but also gives your business' resiliency efforts a boost.

Prioritizes Protection Against Internal Risks

Your BCDR strategy will be rendered ineffective if internal risks are not identified and rectified. That is why it is imperative to have suitable security, backup and compliance solutions that can act as proactive and reactive tools against risks.

Reduces the Burden on Backups

Integrating elements of compliance and security will dramatically reduce threats to your vital data, thus reducing excessive reliance on backups. Additionally, implementing techniques like deduplication will significantly reduce the cost and need for storage by eliminating multiple and unnecessary copies of a file.

Satisfy Data Access and Retention Prerequisites

Limiting access to data by unauthorized personnel is vital from a security and compliance perspective. An employee must be able to access only the data necessary for them to complete a task. This will eventually help your BCDR succeed and comply with relevant regulatory mandates regarding data retention.

How to Conduct a BIA

A single, specific method to conduct a BIA does not exist. It varies from one organization to the next. However, following these 7 steps can help you conduct an effective BIA:

1. Put together a dependable BIA management team

Although identifying and bringing together like-minded individuals with sufficient knowledge and commitment towards BIA management can be challenging, it's vital for the successful implementation of regular BIA and for developing a robust BCDR strategy. This team should include:

- **Executive sponsor/senior manager(s)**

  An executive sponsor or a dedicated senior manager pulls the strings of BIA planning and execution. They ensure that the entire team is accountable for timelines and outcomes.

- **BIA project managers**

  They report to the executive sponsors/senior managers. They must ensure that the tasks are completed correctly and that subordinates are performing as expected.

- **Specialists**

  These are subject matter experts who report to project managers. For example, it could include your organization's security, backup and compliance experts who contribute inputs based on their area of focus.

2. Identify critical processes, systems and vendors

Identify the processes, systems and vendors necessary to support operational continuity. Always use an **objective criterion** to find out what is important and overcome personal biases.

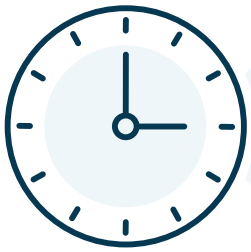
A critical function can be identified by answering these questions:

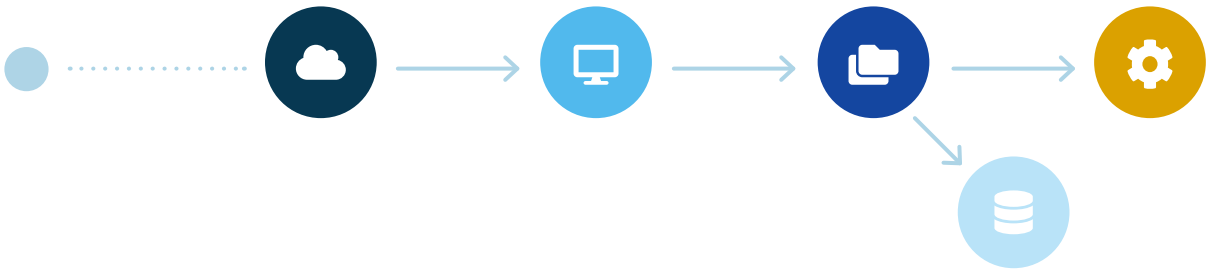
- **Does the function support any business objectives?**
- **How often is the function executed?**
- **Are there any departments dependent on this function?**
- **Does the completion of this function depend on other functions?**
- **Are there other functions that depend on this function for completion?**
- **What would be the revenue loss if this function comes to a standstill?**
- **Will discontinuity (downtime) of this function lead to any compliance violations?**
- **Will fines, lawsuits or other punishments be levied if this function is not operative?**
- **Is the market share or reputation dependent on this function?**

3. Establish recovery timeframes

Evaluate the RPO, RTO and MAD relevant to your business. To minimize opportunities for error in calculating these essential metrics, it's advisable to enlist expert help **(including your IT team)** to get accurate recovery timeframes.

Think about how long your business can tolerate disruption to key processes, systems and vendors without serious financial loss. Then think about possible approaches to get them back on track and the time it would take. This will give you your recovery timeframes.





4. Track the flow of sensitive data

It's imperative to track all business-critical data, irrespective of whether it is at rest or in transit. You must have clarity on even the smallest chunk of sensitive data being generated, stored or transmitted by your business.

A good way to determine the flow of sensitive data is through data flow maps. These maps can be drafted by using your network diagram as a reference. It represents sites with symbols to highlight the vital network devices involved. For businesses with sensitive data at multiple sites, a high-level diagram is recommended. This approach helps make data flow more comprehensible.

5. Determine the monetary and non-monetary impact of an incident

Determining the impact of a disruption in monetary and non-monetary terms is vital. Apart from the obvious financial loss, even loss of reputation, for example, could lead to permanent closure.

Estimating the monetary and non-monetary impact of disruption helps you calculate the total loss incurred by your business.

Total loss incurred = Loss of revenue + Loss of productivity + Recovery-related costs + Intangible costs *(for example, loss of market share)*

6. Sort processes and systems based on their necessity for business continuity

In this stage, you must prioritize the most vital processes and systems over others. Protecting these essential processes during a disruption dictates how well your business operates during a crisis.

7. Draft a roadmap for BCDR

Use the results from BIA to develop a BCDR strategy that suits your business needs. The strategy must be comprehensive by taking into consideration the current threat landscape and possible future threats.

Impact Analysis Matrix

Once you understand which assets are critical to the business and what the potential impacts of disruption are, you can develop an impact analysis matrix. This can be done initially with a simple spreadsheet.

Let's begin by assuming that we are trying to plot a matrix with three considerations — threshold time after a disruption, operational impact and financial impact. The matrix would look like this:

Threshold Time After a Disruption	Operational Impact	Financial Impact
This is the time beyond which the disruption would have a severe impact. (30 minutes, 1 hour, 24 hours, 48 hours, 1 week, etc.)	List the operational impacts that you would face beyond the threshold time. (Customer dissatisfaction, regulatory fines, loss of sales, increased expenses, etc.)	Calculate the operational impact in monetary terms to get the corresponding financial impact.

Employee and Contractor Training

An enormous gap in most security, backup or compliance programs is employee/contractor training. Regular training matters because insider threats are increasing at an alarming rate. What makes the situation worse is that these threats are hard to detect.

The Growing Impact of Insider Threats

The number of insider incidents has increased by about

50%

since 2019.[2]

About 60% of organizations suffered over 30 incidents per year.[2]

It takes an average of over

2 months

to contain an insider incident.[2]

Small organizations spend an average of over

$7.5 million

per insider incident.[2]

Communicate insights from your BIA via regular training sessions. For example, once you identify the business-critical functions, create a training session based on that, emphasizing what employees should or should not be doing to protect system uptime.

Measure the impact of these training sessions by tracking increases or decreases in the number of insider incidents, etc.

5 Ways to Make BCDR Training More Effective

Here are a few ways to make training for employees, contractors and vendors more effective:

1

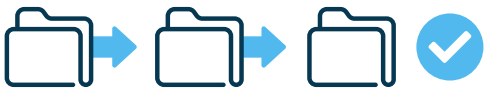
Make training sessions interactive

Make sure that the training sessions are interactive and, if possible, in a video format. You can provide textual content as a complimentary piece. Always make sure the session allows participants to clarify doubts.

2

Break the content into modules.

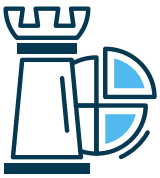
Break the training content into smaller modules so it has a better chance of retention than a lengthy piece of content. Consider keeping training sessions to 30 minutes or less and making sure that every topic within a session is completed in less than five minutes. Once the training is completed, remember to provide a certification.



3

Facilitate self-paced learning

Give pupils the freedom to learn at their own pace and set deadlines based on topic complexity.



4

Include relevant material

The learning content must not include irrelevant and obsolete content. You must update it regularly keeping in mind the rapidly changing cyber landscape.

5

Conduct quizzes and simulated drills

To test the knowledge and awareness imparted by the training, conduct quizzes and simulated drills after every session.

Partner for Success

Regardless of the industry or country in which you operate, your organization can benefit from using a BIA to identify critical business functions, quantify the impact of disruptions and draft a BCDR strategy. Remember that an effective BIA can act as a foundation for business resiliency and continuity. However, if you are not sure whether you can handle producing a BIA on your own, we can fill in the gaps.

Contact us to learn more and let us help you make your BIA journey easy and effective.

References:

1. Cybersecurity Ventures
2. 2020 Cost of Insider Threats: Global Report