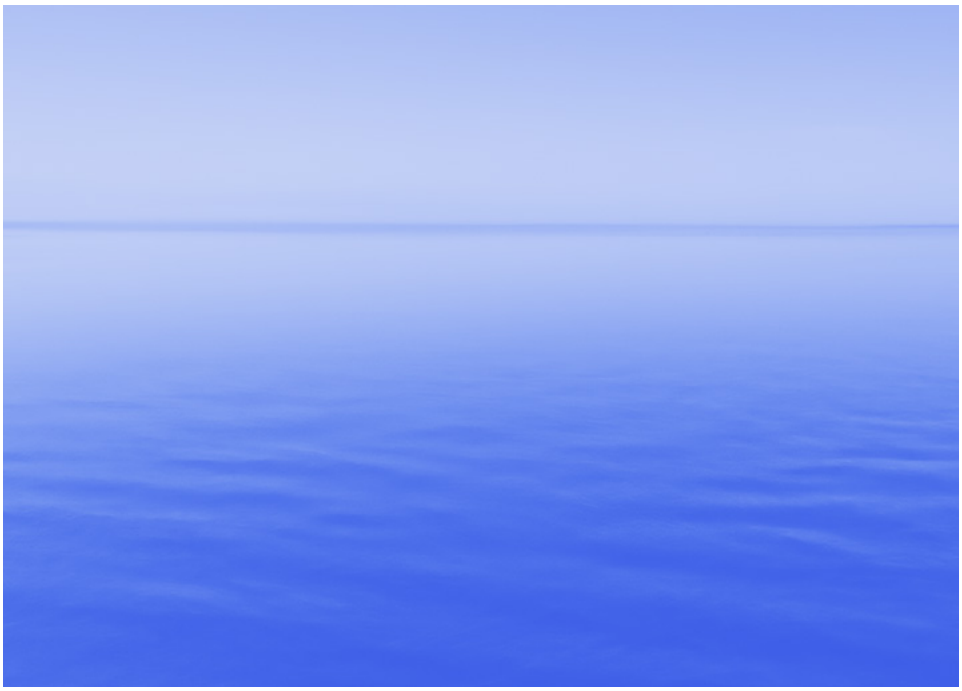
Clearwater

Whitepaper

Business Impact Analysis (BIA): Key to Organizational Resiliency

10 Steps to BIA Success

Table of Contents



Introduction

In the healthcare industry, change is constant, and that may never have been clearer than during the Coronavirus pandemic.

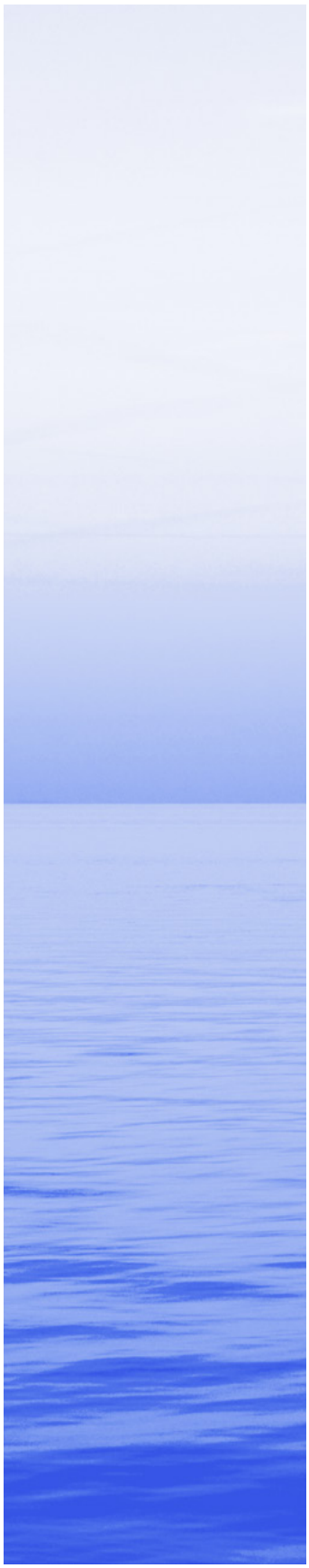
The COVID-19 outbreak changed how the world does business, and that's especially true for healthcare organizations. As the result of adapting environments fueled by social-distancing and stay-at-home mandates, healthcare was forced toward innovation adoption, and digital transformation rapidly emerged as an industry-wide priority, pushing the need for virtual care and telemedicine options to the forefront.

That shift tested organizations' steadfastness, with clinical resiliency front-of-mind for healthcare entities of all sizes and focus. It was particularly challenging for IT, privacy, and security professionals who were forced into rapid adoption and implementation of new technology-supported delivery models—models that moved away from traditional, disjointed operations with singular focus on electronic medical records (EMR) systems to more unified, efficient delivery methods.

Those changes brought with them a range of new risks and potential attack vectors, as we saw cyberattacks increase during the pandemic, highlighting the need for strong cyber risk management programs for both healthcare covered entities and business associates. Many organizations learned they can no longer approach cyber risk management with a check-box approach for compliance. Risk analysis and risk management are tied to patient care and safety, making them a priority for all.

Unfortunately, these rapid changes in telehealth and technology adoption highlighted some industry-wide inefficiencies, especially when it comes to preparedness for disruptive events or disasters. In fact, the pandemic and the rise of successful ransomware attacks exposed major issues for U.S. healthcare in terms of preparedness.

Some of the attack successes and issues with preparedness may be directly tied to the emerging technological dependencies across healthcare entities. With so much rapid innovation, it's becoming even more clear that modern healthcare organizations can no longer exist without a supporting technical ecosystem. That's even true beyond inner-operations and extends into the supply chain,



where the pandemic highlighted a growing number of operational-critical pain points and the importance of risk impact understanding for business continuity and disaster response planning.

The pandemic has also highlighted the critical role leadership teams play in effective planning and preparedness, from making decisions about risk thresholds to ensuring teams have adequate resources and financial support to ensure operational resilience.

But one of the most important lessons from the pandemic may be the importance of effective Business Impact Analysis (BIA) for business continuity and disaster recovery planning—not just for compliance and regulatory requirements, but also as a best practice for survivability in this changing environment and new normal of doing business.

> "The Business Impact Analysis engagement with Clearwater surpassed our expectations."
>
> Jeremy Singleton, Information Security Director, U.S. Anesthesia Partners (USAP)

Understanding business impact analysis

Some of the challenges with disparate preparedness and risk impact understanding may arise when organizations do not understand what a BIA is or what it entails.

A BIA is a blueprint that informs your business decisions. It helps build your organizational preparedness and guides your business continuity management.

Your BIA brings your business goals and objectives into IT operations and gives your business leaders a seat at your business continuity table.

An effective BIA embodies your organizational processes that identify your most critical business activities and associated resources to ensure operational resilience during and after a disruptive event.

Essentially, your BIA helps your organization build business continuity and disaster recovery plans around the needs of your business. It unifies your programs (for example, your business continuity, disaster recovery, crisis management, incident response, and contingency plans) for a similar big-picture objective—to remain operational when faced with a disruption or disaster. All of these may be separate

plans and some of them may be managed by separate areas of your organization, but they all fit together and they should be based on your business needs.

Unfortunately, for many organizations their business continuity and disaster recovery plans are not built around the needs of the business. They're not updated or tested, and many don't include pandemic situations or cyberattacks, even after lessons learned from 2020.

Many organizations also do not have updated BIAs, which is a critical component for business continuity and operational resilience. Your BIA brings business requirements into IT operations by providing visibility into critical business processes and helping to build an up-to-date IT system inventory, which is critical for business continuity and disaster recovery.

> "Beyond simply documenting the information required in order to begin creating a business continuity plan, this work facilitated a thorough comprehension of our business processes and the underlying critical capabilities that supported them."
>
> Jeremy Singleton, Information Security Director, USAP

More than 90 healthcare organizations in the United States suffered a ransomware attack in 2020, almost double from the previous year. And these attacks aren't just growing in frequency, but they're increasingly more sophisticated and result in millions of record exposures in just a single attack.

Prioritizing functions and processes to meet your mission

As we've mentioned, an important component of BIA success begins with identifying your organization's mission and aligning that with your business continuity and disaster recovery plans. That includes identification of your primary business functions and supporting business processes, as well as an understanding of the impact on your operations if a function or process isn't available.

What does this look like in a healthcare setting? Here's an example:

- In a healthcare organization, a primary business function might be something similar to finance or accounting.
- A key process of accounting or finance as a primary business function would be payroll.
- Here, we need to look at both the qualitative and quantitative impact on the organization if unable to do payroll.
- From a qualitative perspective, if your organization lost the ability to issue payroll, at the highest level, we wouldn't expect a severe impact such as loss of life, however, they may be a significant financial impact.
- From a quantitative perspective, if you're not able to do payroll there may be a cost to the business, which you would need to rate over a period of time.

Next, you should determine which resources your organization needs to support these most critical business functions and processes.

Here's an example in a hospital setting:

- The hospital's mission (it's essential function) is to provide quality care.
- One of its primary business functions is its emergency department.
- Examples of business processes performed in the emergency department could include triage and registration.
- Your team needs resources to perform triage and registration. For example, a triage nurse (staffing/personnel) and also medical equipment (for example to check vitals). There are also specific systems needed for triage and registration that are process dependent, such as the EMR system.
- Next, you should evaluate the maximum allowable downtime (MAD), which helps

quantify how quickly you must recover a business process during a disaster. Your MAD may be influenced by factors such as your ability to provide a reasonable level of service through alternative means; financial impacts; and other intangible impacts such as a loss of customer confidence.

- In addition to your MAD, you must also have a good understanding of both your recovery time objectives (RTOs) and your recovery point objectives (RPOs). While there are some commonalities between the two, they are different. Your RTO determines how quickly you must recover supporting systems to support a business process. Your RPO determines how much data loss you can tolerate before significant business process impact. Remember, the date of your most recent data backup or snapshot, located off-site, affects your maximum allowable data loss, and both RTOs and RPOs are customizable and unique to your individual organization.

Using a BIA for better business decisions

A Business Impact Analysis has many benefits. While some people believe that a BIA only captures system information, it actually gives you so much more information, which you can use to make better informed business decisions.

In short, your BIA is a great way to engage your business and IT units with an opportunity to educate with cross-collaboration and develop stronger working relationships.

From a business perspective, your BIA helps you engage your business teams by gauging your operations, identifying gaps, and defining expectations about gap remediation. It helps you identify and address core areas such as:

- Business functions
- Business processes
- Essential personnel
- Dependencies
- IT systems

From an IT perspective it can support you with understanding:

- IT system inventories
- Tier systems

- Data flows
- Essential system SMEs
- Current recovery

> "In all actuality, it would have been very advantageous for us to have done this project with Clearwater much earlier because now I have a much clearer understanding of my organization."
>
> Jeremy Singleton, Information Security Director, USAP

The BIA process, a step-by-step guide

So, now that you have a better understanding of what a BIA is and how it can help ensure operational resilience for your organization, you may need a little help with some tips on how to conduct an effective BIA. Here are 10 recommended steps to consider for BIA success:

Step 1: Validate your organization's mission-essential functions to guide the process

Step 2: Determine the scope of business functions for your organization. Think in terms of departments or divisions. Ask, which departments/locations/divisions should be included as part of your Business Impact Analysis? Make a list. There may be more than you initially realize. A hospital system, for example, could encompass 30 departments or more.

Step 3: Determine which key stakeholders and/or business leaders who need to be involved in your BIA and then schedule a project kick-off meeting. During this meeting, explain what the project is, why you're doing it, how it benefits the business, and what the expectations are for participants.

Step 4: After the kick-off meeting, send out business process pre-work, which are generally questionnaires. This is a tool to collect important data. In our experience, in some organizations, some business leaders may struggle with the questionnaire. A stumbling block may be created by a narrow focus on systems when they should

focus on key processes instead. Try to keep your participants focused on about five high-level processes to keep them out of the weeds.

Step 5: Once your participants have completed the pre-work, schedule and conduct follow-up interviews. These interviews will help you validate the information they've shared and can help you understand their answers with assurance they've included everything you need.

Step 6: Analyze results and prepare a findings report.

Step 7: Share report results with stakeholders.

Step 8: Address gaps identified by the questionnaire and interviews. What is the bridge between needs and capabilities?

Step 9: Update your BIA whenever your environment changes.

Step 10: Perform a comprehensive BIA at least every three years, more frequently if applicable and possible.

Ingredients for BIA success

When it comes to BIA success and value, it's important early on to understand roles and responsibilities. While this is not an encompassing list, it's a great starting point.

1. Senior leaders

This is where you will get your executive sponsor—the person authorizing and supporting your BIA, your program champion. If you have trouble getting people to participate or if you have issues identifying key departments and leaders, your executive sponsors should step in and help.

Your senior leaders also play an important role by assuming responsibility for ensuring that your continuity plans are sufficient and will sustain the business in the event of a disaster.

By authorizing and supporting your BIA process, senior leadership will take the first step toward informed disaster recovery planning.

2. Business leadership

Your business leaders will participate in BIA pre-work and your BIA interviews. These leaders should understand the impact of disruptions on your business operation, especially if business critical processes are temporarily unavailable.

3. System owners or subject matter experts (SMEs)

By involving systems owners and SMEs in your BIA, they can provide additional perspectives and context, especially about how your organization uses critical systems to perform processes. They can also provide additional insight into the impact on business operations when information systems are not available and manual processes must be implemented. Your SMEs can also help formulate efficient and effective mitigation strategies.

While individually each of these groups have important roles, a successful BIA requires engagement from all three.

Outcomes of a successful BIA

When it comes to effective BIA processes, the resulting outcomes are truly a blueprint for building resilience plans around your business continuity and disaster recovery programs.

Here are some examples of successful BIA outcomes:

- Identification of mission essential functions (MEFs): This is the limited set of functions your organization must continue throughout or must be resumed rapidly after a disruption or disaster.
- Identification of business functions and specific processes: These are functions and processes your organization must conduct to perform your MEFs. They are enablers that make it possible to perform your mission.
- Assessment and prioritization of business functions and processes.
- Identification of systems and applications used to perform the mission and business processes.
- Maximum allowable downtime (MAD), the amount of time the business function can be down before considerable impact to the mission.
- Recovery time objectives (RTOs), the amount of time after which you must recover supporting systems.
- Recovery point objectives (RPOs), the amount of data a business unit can afford to lose due to an outage.
- Specific business function information regarding key personnel, normal work hours, peak periods, vital records, and dependencies.

- Validation of disaster recovery and business continuity efforts, including identification of non-essential functions and roles so you understand what you can suspend and what needs your attention most. You can use the BIA to better understand why you included certain elements in your plans and if they functioned as designed.
- Updated contact and other important information for key business leaders and departments.
- Identification of primary operations and locations.
- Identification of IT systems necessary to support primary business functions.
- Vendor services and supply needs to support primary business functions
- Internal and external dependencies for primary business functions, including supply chain

Key takeaways

While the list of benefits of a BIA for your organization are many, here are a few key BIA takeaways to consider and share with other members of your team. Your BIA should:

- Prioritize mission/business processes
- Identify risk mitigation and recovery strategies based on criticality
- Identify resources needed to resume mission/business (facilities, personnel, equipment, software, data files, system components, vital records)
- Identify dependencies (suppliers, third-parties, data feeds, interfaces)
- Validate and inform IT system inventory
- Inform an overall risk management program
- Build “enhanced resilience” (Health and Public Health Critical Infrastructure)
- Allow for informed decisions for business continuity/disaster recovery planning (such as budget, resources, etc.)

Are you interested in learning more about the role of a Business Impact Analysis in risk management or want to take a closer look at how you can improve or mature your existing BIA processes? Clearwater has a number of free BIA-related resources for you. Here are a few you may want to explore:

Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact