



Business Continuity Starts with a Business Impact Analysis

Identifying and assessing critical processes, people,
and priorities to ensure resiliency, strength,
and market confidence





Contents

Introduction3

 Business Continuity Management Moves Center Stage3

 Expectations vs. Reality in 20203

Business Resiliency Overview4

 Building Market Strength and Organizational Confidence.....4

 Business Impact Analysis (BIA):.....4

 Recovery Strategies:4

 Business Continuity Plans:4

 Testing:4

 Ongoing Monitoring:4

Business Impact Analysis..... 5

 What is a Business Impact Analysis and Why is it Important? 5

 Identifying Operational & Financial Impacts5

Conducting Your Business Impact Analysis6

 BIA Four Phases8

 Phase One: Prepare9

 Phase Two: Gather10

 Critical Business Processes.....10

 Critical People10

 Critical Applications10

 Critical Third Parties10

 Critical Infrastructure10

 BIA Input Tracker & Analysis Tool.....10

 BIA Interview Best Practices11

 Data to Collect During Interviews11

 Phase Three: Analyze12

 Identify Components.....12

 Identify Risks12

 Phase Four: Report & Recommend14

 Sample Risk & Resiliency Priority Chart15

 Conclusion16

 About CyLumena16

 BIA Glossary.....18

 Resources.....18

Introduction

Business Continuity Management Moves Center Stage

The medical and social events of the first half of 2020 have revealed the value of business resiliency in the face of any disaster or disruption, no matter the cause.

A recent study found that 66 percent of UK organizations surveyed had no pandemic plans before COVID-19ⁱ despite a pandemic ranking highest in terms of impact and likelihood in the UK government’s National Risk Register of Civil Emergencies. Despite this apparent gap, a surprising 61 percent of respondents indicated that they consider their business continuity ‘up-to-date.’

Regarding the United States, a different study found that while 56.8 percent of businesses had a pandemic-specific plan, fewer than 50 percent had a generic contingency plan and over 10 percent had no plan at all.

The pandemic highlighted that many companies have limited visibility into their risk exposure or supply chain, particularly among tier two and three suppliers that provide key components and deliverables. ⁱⁱ

Additionally, companies are realizing more today than ever that they have a responsibility to their customers, employees, and community to be successful both in financial and societal terms and regarding the interdependencies among stakeholders. Breakdowns of critical business services impact more than revenues, profit, and reputation. They damage relationships over the long run and have cascading impacts on broader market participants and social structures.

Expectations vs. Reality in 2020

It is striking how much our view of business resilience and continuity planning can change in the face of global disruption. For instance, the Business Continuity Institute (BCI) conducted a significant ‘Trends and Challenges 2020’ survey in late 2019 that indicated 64.6 percent of business continuity professionals were expecting to see only relatively small changes to the way their organization would manage business continuity during 2020, while just a third of the professionals were planning significant changes.

Since the results of that survey were released in early 2020, the COVID-19 pandemic has changed the way businesses function, both temporarily and permanently. The full scope of future changes is yet to be revealed.

BCI’s research and report on the pandemic found that only 24.8 percent of businesses expect to ‘go back to their old business model,’ demonstrating the immense impact the coronavirus has had on businesses and the need for organizations to change at rapid speed to ensure survival. ⁱⁱⁱ

Many businesses have moved online, some have remodeled their supply chains, and others have started manufacturing and marketing completely new products – all examples of how organizations must be creative to ensure their post-pandemic existence.

Whether an organization was well-prepared for the probability of a pandemic or it had no contingency plan in place for any business disruption or disaster, organizational leaders have seen the fragility of business systems, operations, and revenue streams and witnessed the critical importance of risk awareness and preparedness.

While the pandemic is a once-in-a-lifetime event, risks of all types are increasing, and the global nature of the economy can impact any business without warning.

Business Resiliency Overview

Building Market Strength and Organizational Confidence

Business Resiliency, also known as Business Continuity Management (BCM), exists to prepare an organization for inevitable disruptions, emergencies, and disasters. These disruptions may be caused by internal or external, local or global, and natural or human-created events; however, the value of planning is to preserve the organization by minimizing risk and damage. The benefits of planning are apparent when an organization demonstrates the confidence to face uncertainty, maintains standards that persist, and sustains operations that can flex and adapt quickly. A resiliency-focused planning lifecycle creates a strength that provides market value, competitive advantage, and customer confidence.

Figure 1 highlights the four phases in a business resiliency lifecycle.

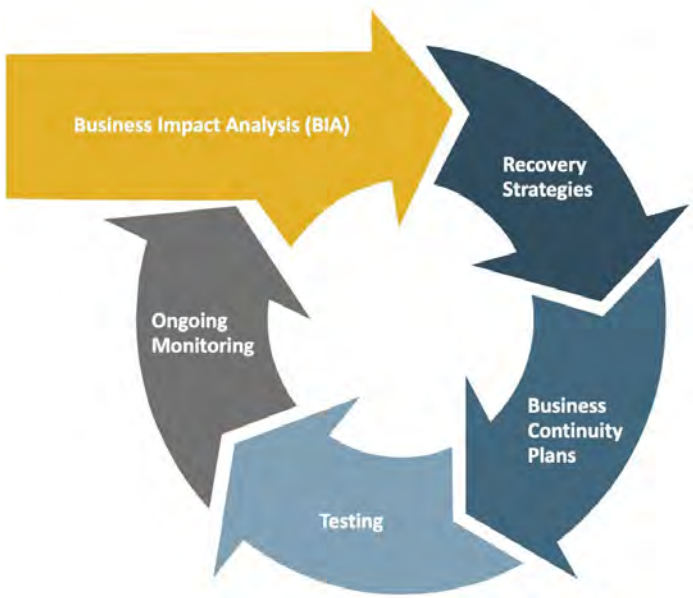


Figure 1: Business Resiliency Lifecycle

Business Impact Analysis (BIA):

Identifies critical business functions, predicts the consequences of disruption, and obtains information required to develop recovery strategies and limit the potential loss impacts.

Recovery Strategies:

Creates the plans needed to restore business operations to a minimum acceptable level following a business disruption by prioritizing the Recovery Time Objectives (RTOs) developed during the BIA.

Business Continuity Plans:

Outlines all procedures and instructions an organization must follow when facing a disaster. Addresses business processes, assets, human resources, third-party dependencies, and others.

Testing:

Analyzes recovery strategies, controls, and plans to ensure that they function as intended. Standard tests include tabletop exercises, structured walk-throughs, and simulations.

Ongoing Monitoring:

Promotes the effectiveness of the business resiliency program by periodically reviewing and updating recovery strategies and business continuity plans to improve the organization’s risk posture amid powerful influences.

The balance of this white paper will focus on the first phase of the Business Resiliency Lifecycle – the Business Impact Analysis – and how a proper BIA creates full transparency to the organization’s current risk landscape and enables leadership to carry out the remaining phases.

Business Impact Analysis

What is a Business Impact Analysis and Why is it Important?

The Business Impact Analysis (BIA) is the first and most critical step in an organization’s Business Resiliency Lifecycle (Figure 1). The purpose of the BIA is to identify the company’s essential functions and any potential risks to those functions while providing the critical information required to create Business Resiliency and Disaster Recovery plans in the future lifecycle phases.

Creating a BIA requires uncovering and assessing the general and specific risks to an organization.

The BIA process allows each department or business unit to explore how unexpected events could affect each business function. Then, the organization uses this gathered intelligence to prioritize specific functions

through the calculation of key metrics, including: Recovery Time Objective (RTO), Recovery Point Objectives (RPO), and Maximum Tolerable Downtime (MTD). These measures (see BIA Glossary on page 18) ensure that data, rather than assumptions or politics, drive an organization’s continuity and risk-mitigation priorities.

Identifying Operational & Financial Impacts

A comprehensive BIA identifies the operational and financial impacts caused by business disruption. The chart below shows the eight areas that should be reviewed and their potential effects assessed across each type of risk or potential disruption.



Why is the BIA important?

- Pursues Effective Risk Management
- Prioritizes Enterprise Tools & Resources
- Promotes Investment by Key Stakeholders
- Enables Operations Optimization
- Supports Continuous Risk Monitoring
- Creates Optimal Readiness
- Fosters Compliance
- Supports Best Business Practices
- Facilitates Corporate Citizenship



Organizational leaders have seen the fragility of business systems, operations, and revenue streams, and witnessed the critical importance of risk awareness and preparedness.

Conducting Your Business Impact Analysis

As previously mentioned, a BIA identifies a company's critical business functions. The BIA also predicts the likely consequences of a disruption or disaster, and

it provides the vital information needed to create the Business Resiliency and Disaster Recovery plans in future business resiliency phases.

Figure 2 highlights six outputs and types of information that make a BIA an invaluable step in business resiliency and continuity.

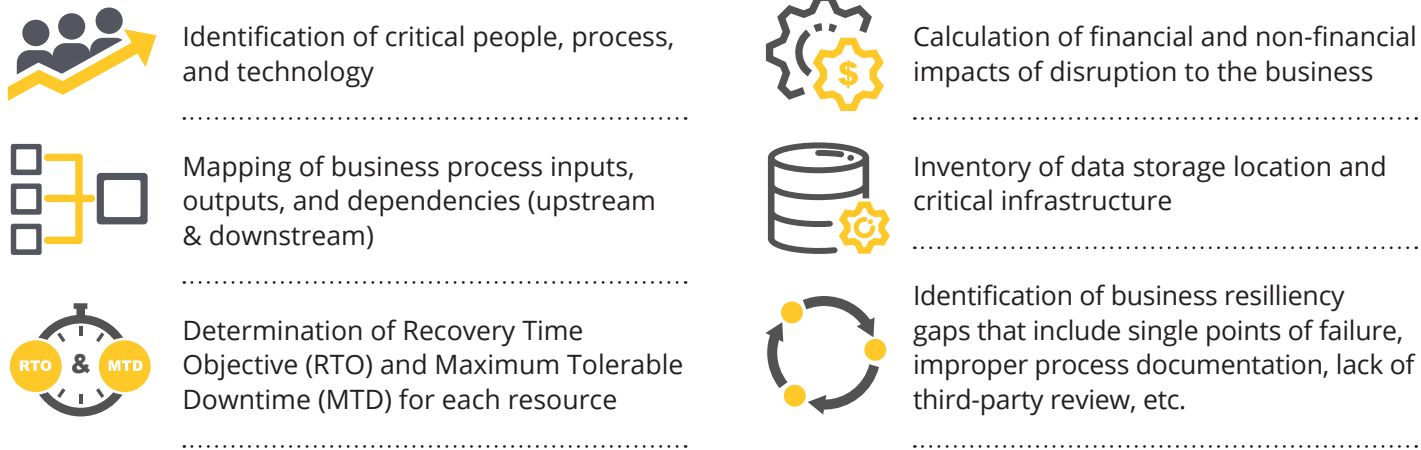


Figure 2: Six outputs that make BIA a valuable tool.



Four Phases


Phase One: Prepare


Phase Two: Gather


Phase Three: Analyze


Phase Four: Report and Recommend

Business Impact Analysis

- 

Kick off the BIA process by gathering and educating stakeholders and gaining cross-functional commitment from senior leadership. Communicate the value of BIA, create an execution plan and schedule, as well as align on the path forward.
- 

Most of the effort is carried out in this phase; collecting many data points and input sources needed to conduct a robust BIA. Thoroughly document all relevant criteria for each process, application, and dependency. Data for analysis will cover five critical functions.
- 

Conduct a thorough analysis to identify risks and the organization's most critical components, as well as establish the priority level of essential processes, applications, third parties, and required infrastructure.
- 

Document all collected data and the results of the analysis. Provide recommendations for mitigating uncovered risks. Disseminate reports and recommendations, as well as communicate with relevant stakeholders and executives to ensure alignment on mitigation plans.

Phase One: Prepare

Focus: Communication with Leadership

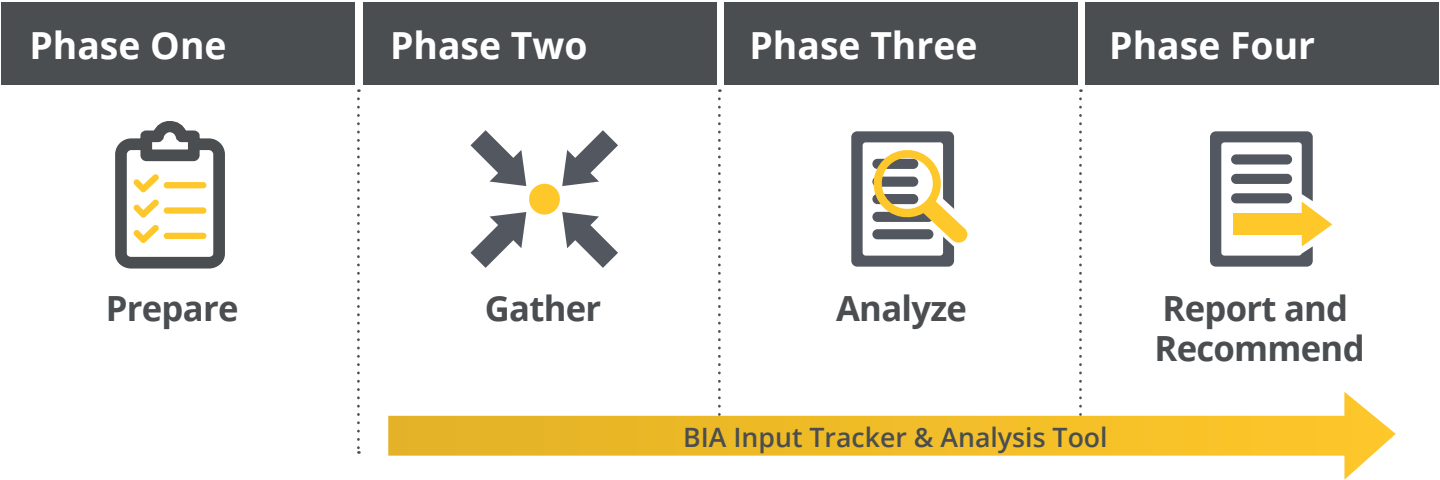


Figure 3: Four phases to conduct a Business Impact Analysis.

- A Business Impact Analysis is useful when an organization has a cross-functional commitment from senior leadership. That commitment cascades throughout each business unit and ensures that process owners, application owners, third-party owners, and infrastructure managers prioritize their efforts throughout the BIA process. Kicking-off a BIA process requires that the Business Resiliency team meet with applicable senior leadership and project stakeholders to carry out six steps:
1. Communicate the value and importance of a BIA (Note: This white paper can be a helpful first step.)
 2. Understand the organization's current risk environment
 3. Identify which business units, departments, or lines of business should be included in the BIA scope
 4. Socialize and align on the approach to and execution of the BIA
 5. Finalize the execution plan and next steps
 6. Establish the BIA project schedule

Key to a successful BIA is education, communication, and alignment with key leadership and stakeholders throughout each phase, but particularly in Phase One.



Phase Two Must-Have

BIA Input Tracker & Analysis Tool

Phase Two is smoother, and the output is easier to assess and report on, when the input is gathered via a standardized tool or technology.

While there are software tools and services that aid in the gathering, documentation, and analysis of BIA inputs, any consulting firm that provides BIA support and facilitation should provide a tool for this purpose.

Any tool should meet the following best practices:

- Provides a standardized mechanism for the collection of all relevant BIA data
- Provides a mechanism for calculating potential loss impacts
- Enables aggregation and analysis of data across all organizational business units
- Gives detailed instructions and definitions for all data fields
- Organized so that process owners, application owners, infrastructure owners, third-party owners, and critical resources can populate their respective data separately, and the tool will automatically create relationships among the datum
- Available for future BIA analysis to enable trend analysis over time

Phase Two: Gather

Focus: Collect BIA Inputs

After the preparation phase is complete, the task of collecting the many data points and input sources is needed to conduct a thorough BIA. Phase Two is where the bulk of the effort is invested when conducting the BIA. It is essential to thoroughly document all the relevant criteria for each process, application, and dependency.

There are five critical functions around which the BIA process will collect information for analysis:



Critical Business Processes

These are the foundational processes that must be restored promptly after a disruption to ensure that assets are protected, meet fundamental operational needs, and satisfy mandatory regulations and requirements.



Critical People

These are the human resources required to support critical business processes and fundamental functions.



Critical Applications

These enterprise or departmental tools, software, and platforms support critical business processes and people's roles and functions.



Critical Third Parties

Third parties are outside organizations, partners, and vendors that support critical business processes, functions, and deliverables.



Critical Infrastructure

These are physical, technological, and services that support critical business processes, operations, and functions.

Phase Two Best Practice

Mastering the BIA Interview

Many BIA consulting firms provide forms or spreadsheets for their clients to capture the critical inputs that the BIA requires to be effective. However, using individual or group interviews is the most efficient method for collecting this valuable information from stakeholders. Interviews ensure a more robust BIA as interviewers can ask follow-up questions that spreadsheets can't.

Best Practices for Conducting Compelling BIA Interviews:

- The interviewer should provide a detailed overview of the BIA, its purpose, and expected outcomes and purpose of the interview.
- The interview should be conducted as a partnership between the interviewer and interviewee. The goal is not to point fingers but to capture all relevant data to ensure that risks are identified so that they can be mitigated, reducing the organization's risk posture.
- The interview should be conducted "live," ensuring that the interviewer can facilitate the conversation, answer questions, and document results in real-time.
- Interview results should be captured in a BIA Input Tracker and Analysis Tool to facilitate consistent and accurate data aggregation and analysis. See page 10 for best practices.

An experienced interviewer can confirm, uncover, and validate critical functions and priorities.

For many organizations, the interview-based input collection approach brings greater context to understanding the business and their dependencies and reveals far more critical processes.

- Once the interview has been completed, all information should be populated into the BIA Input Tracker and Analysis Tool and shared with the interviewee. This will allow the interviewee to review all material and ensure complete answers.

Data to Collect During Interviews

Individual and group interviews are most useful for identifying critical functions across the organization and gathering needed facts. These interviews should be conducted with each business unit to recognize vital functions across the organization and any relevant criteria about each. Utilizing a BIA input tracker and analysis tool or technology is essential.

What Data Should Interviews Collect?			
Critical Business Processes <ul style="list-style-type: none">• RTO• MTD• Inputs & Outputs• Upstream & Downstream Dependencies• Peak Periods or Seasonality• Manual Workarounds• Remote Capabilities	Critical Applications <ul style="list-style-type: none">• RTO• RPO• Critical Business Processes they Support	Critical Infrastructure <ul style="list-style-type: none">• RTO• RPO• Critical Business Processes they Support	
Critical People <ul style="list-style-type: none">• Critical Employees	Critical Third Parties <ul style="list-style-type: none">• RTO• RPO• Critical Business Processes they Support	Potential Loss Impacts <ul style="list-style-type: none">• Financial: Lost or delayed revenue, regulatory fines, increased Expenses, contractual penalties• Non-Financial: Reputation, contractual obligations, legal and/or regulatory liability, customer service, employee morale, financial reporting	

Phase Three: Analyze

Focus: Assess Risks, Likelihood & Impact

Once all applicable information has been documented, Phase Three focuses on conducting a thorough analysis to identify the organization's risks, identify the most critical components of the organization, as well as determine the priority level of essential processes, applications, third-parties, and required infrastructure.

Identify Components

Phase Three analysis should identify the most critical components of the organization based on the following criteria:

- Number of Critical Processes supported
- Supports the highest number of Critical Business Processes
- Number of business units that utilize the highest number of applications, third-parties, and/or infrastructure
- Sensitive data points accessed
- Related to regulatory requirements
- Customer-facing
- RTO
- RPO
- Impacts or increases financial or reputational risk

Identify Risks

Phase Three analysis should identify risks to the organization and determine the likelihood and impact of those risks. The most common risks uncovered in Phase Three include:

- Single Points of Failure:** Process involves critical individuals with unique knowledge.
- Processes with No Remote Capabilities:** Process cannot be performed remotely and requires the use of company buildings.
- Processes with No Manual Workarounds:** Process possesses a reliance on applications to be completed.
- Procedures Requiring Specialized Equipment, Hardware, or Infrastructure:** Process relies on specific equipment to be completed.
- Operations with a Dependency on Third-Parties:** Process relies on a third-party technology or service to be completed.
- Lack of Sufficient Process Documentation:** Processes are not adequately documented and/or there is no standardization for documentation.
- Lack of Employee Training:** Employees do not have a foundational understanding of Business Resiliency and its components. Example: employees often think that having business continuity plans is sufficient.
- Understaffing:** Many organizations do not view business resiliency as a priority and, as a result, do not appropriate dedicate staff to support.



Phase Four: Report & Recommend

Focus: Document Results & Make Recommendations for Risk Mitigation

After the analysis has been carried out, Phase Four focuses on documenting the collected data, analyzing results, and providing recommendations for mitigating uncovered risks. Conclusions, reports, and recommendations should be socialized with relevant stakeholders and executives to ensure that risks are clear and that key leaders are engaged in mitigation plans.

BIA Report Should Address These Areas

Processes, Applications, and Infrastructure are broken down by RTO

- RTO should be broken down in time increments of <4 Hours, 8 Hours, 24 Hours, 48 Hours, >72 Hours
- These section outlines which processes should be prioritized in the event of an incident

Processes, Applications, and Infrastructure are broken down by RPO

- This section highlights where the most critical data resides and helps prioritize restoration in the event of an incident

Risks to the Organization

- Identifies various risks to the organization gathered from interview data analysis, including common risks:
 - > Single-Points-of-Failure
 - > Lack of remote capabilities
 - > Lack of manual workarounds
 - > Lack of redundancy
 - > Specialized infrastructure
 - > Overreliance on third parties

Critical Business Units

- Identify those business units most critical based on data gathered and risks uncovered

The BIA report should present analysis highlights and outline recommendations in the form of a mitigation strategy and roadmap to address identified risks and mature the business resiliency program.

This report provides critical information required to move into the next phases of the business resiliency lifecycle, including Business Resiliency and Disaster Recovery plans.

Figure 4 on page 15 shows a Risk and Resiliency Priority Chart, using color coding to indicate level of risk and effort to mitigate.

Sample Risk & Resiliency Priority Chart

Notable Risk Mitigation	Risk to Organization	Level of Effort
Leverage the Business Resiliency Steering Committee to promote resilience initiatives across all Business Units	High	Low
Review Third-Party Business Continuity plans based on risk rating and criticality as 70% of critical processes depend on at least one third party	High	Moderate
Address the 25% of processes that demonstrate a Single-Point-of-Failure that could result in process disruption	High	Low
Review the 47% of critical business processes that do not currently have a manual workaround to identify potential resiliency alternatives	High	Moderate
Review and standardize documentation for all critical business processes. Documentation was only received from half of the departments and Business Units and was mostly in the form of "Desktop Level Procedures"	High	High
Review the 37% of critical processes that rely on a specialized piece of hardware or infrastructure to assess the process's level of reliance and potential alternatives	Moderate	Moderate
Analyze the 10% of critical processes that cannot be performed remotely to identify potentials for remote modification	Moderate	Moderate

Business Resiliency Maturation	Risk	Effort
Review, update, test, and socialize Disaster Recover and Business Continuity plans	High	High
Review RTO's and RPO's (and justifications) for critical business processes	High	High
Assess Financial and Non-Financial loss impacts (loss of revenue, fines, reputation, etc.)	High	High
Perform risk assessments for all critical business processes to identify vulnerabilities and sensitive information	High	High
Assess current staff against required resources to support each critical business process	Moderate	Low
Assess vital records and retention requirements	Moderate	Low
Standardize, document, and maintain all Business Unit names, Applications, and an org. chart for all BU's	Moderate	Moderate
Develop and conduct Business Resiliency training for the organization	Moderate	Moderate
Conduct bi-annual tabletop exercises to prepare the organization for business disruptions	Moderate	High
Implement a tool to support and manage organization's Business Resiliency processes	Moderate	High

Figure 4: Sample chart indicating risks and next steps with priority and level of effort.



Conclusion

The Business Impact Analysis process, analysis, and report are the first and most critical phase in the business resiliency lifecycle. Without it, an organization does not fully understand its current landscape and cannot create adequate Business Continuity and Disaster Recovery plans nor conduct comprehensive testing exercises. Utilizing a BIA, an organization has intelligence and insight into components the organization relies on when faced with a disaster or disruption.

As a cybersecurity consulting firm focused on building clients' security maturity and strength, CyLumena provides expert guidance, facilitation, analysis, and recommendations through the BIA based on the best practices and recommendations in this white paper.

About CyLumena

As one of the largest security consulting firms in the Pittsburgh region, CyLumena was created out of a growing need for reliable cybersecurity technology, support, and expert guidance for mid- and small-sized organizations.

CyLumena's mission is to provide clients with peace of mind around cybersecurity through a cost-effective combination of preparation and prevention that is called CyberLean.

Backed by decades of professional services knowledge, coupled with strategy and execution deployment, CyLumena adds value to reduce cyber cost burden, enhance risk visibility, and improve strength and resilience in the face of increased cyber threats.



p: 412.251.0848
m: solutionsdesk@cylumena.com
w: cylumena.com



BIA Glossary

Recovery Time Objective (RTO):

The targeted duration of a business process must be restored after a disaster (or disruption) to avoid unacceptable consequences associated with a break in business continuity.

Recovery Point Objective

(RPO): The point in time before a disruption/system outage to which application data must be recovered (given the most recent backup copy of the data) after an outage.

Maximum Tolerable Downtime

(MTD): The total amount of time that the business is willing to accept for a mission/business process outage or disruption and includes all impact considerations.

Process Inputs: Any business units, processes, third parties, hardware, or software that contribute to this process.

Process Outputs: Any business units, processes, third parties, hardware, or software resulting from the process. Customers may be included in process outputs.

Upstream Dependencies:

Any other business units, processes, third parties, hardware, or software on which this process relies.

Downstream Dependencies:

Any other business units, processes, third parties, hardware, or software that rely upon this process.

Critical Employee: One who would significantly impact the organization's ability to conduct regular business if absent. These positions may be managerial, technical, or supportive.

Single Point of Failure: Process involves a critical individual with unique knowledge essential to the process's function.

Remote Capability: A process can be completed outside the office.

Manual Workaround: A process can be completed without the use of a critical application.

Specialized Infrastructure: A process relies on a specific piece of equipment, infrastructure, hardware, or facility to operate.

Third-Party Dependency: A process relies on a third party to operate.

Tabletop Exercise: A discussion-based exercise involving members of each relevant Business Unit, discussing their roles in pre-determined disaster scenarios.

Resources

Continuity Central

ⁱ *"Study finds that two-thirds of UK organizations surveyed had no pandemic plans in place before COVID-19."* May 6, 2020.

Forbes

ⁱⁱ *"Rethinking Business Resilience In The Midst Of The Coronavirus Outbreak."* March 17, 2020.

BCI

ⁱⁱⁱ *"BCI Coronavirus - A Pandemic Response Report 2020."* May 21, 2020.

