

Application / Hardware - Business Impact Analysis Template

The single most important thing we can do is help you understand the criticality of each application, supporting hardware/server/pc and the required network infrastructure, should you experience any type of unplanned disruption. This template is intended to be a high-level summary of your critical business applications, servers, and business functions. It will assist you in accessing recovery options for each application based upon the impact to you business if any of these applications are not available for a specific period of time.

The objectives of this BIA are to:

1. Identify key business and revenue drivers
2. Identify RTO and RPO for essential business functions and processes
3. Identify the impact, if critical business functions cannot operate due to an unplanned disruption
4. Quantify monetary and workflow impacts if critical business functions cannot operate
5. Identify intangible impacts if critical business functions cannot operate
6. Identify high-level minimum acceptable recovery configurations (MARC) and resources required to support critical business functions
7. Identify existing continuity documentation and incident response plans. Review current business continuity preparedness
8. Identify internal and external dependencies such as technology, telecommunications, records and service organizations
9. Recommend strategic and tactical steps required to minimize the impact of an interruption on critical business functions

“MARC” Configuration Requirements

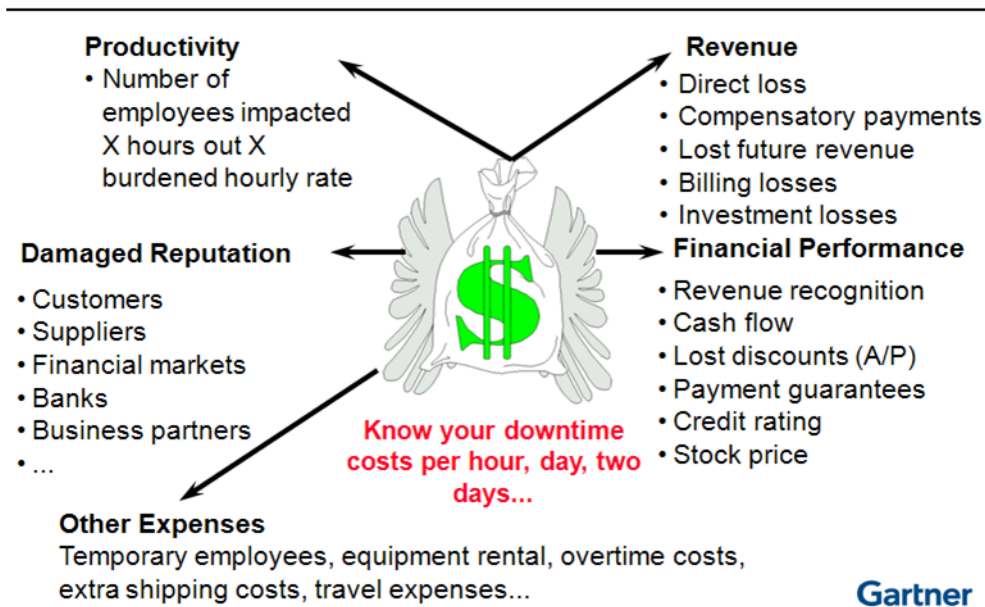
Identify the Minimum Acceptable Recovery Configuration (MARC) requirements, i.e., the high-level facility, equipment, telecom capacities required to continue essential operations for the business areas analyzed.

1. Review the data backup, availability and recovery strategy in place for restoring the essential data
2. Review selected data synchronization/backup solutions to verify that data is readily available and not corrupt to support data restoration and recovery
3. Identify the recovery configuration facilities required to support initial recovery operation, e.g., how many people, what types of space, what equipment and when it is needed for following an interruption
4. Identify non-hotsite alternate processing options that shall meet the recovery requirements (e.g., internal/alternate sites)
5. Identify hardware capacities for subsequent recovery windows (e.g., equipment and facilities, by time, to be acquired and installed at time of disaster)
6. Create written documentation of essential applications and supporting technology (e.g., network, servers, etc) that are required to recover
7. Written procedures for developing equipment acquisitions
8. Written recovery plan detailing what each individuals responsibilities are depending on the type of outage

If the original site must be restored or replaced, the following are some of the factors to consider:

1. What is the projected availability of all needed computer equipment?
2. Will it be more effective and efficient to upgrade the computer systems with newer equipment?
3. What alternative telecom is available to support the recovery process?
4. Is there an alternative site that more readily could be upgraded for business purposes?
5. Is there ample space for personnel to conduct business and required basic equipment; phones, fax, desks, etc

What Is Your Cost of Downtime?



AIMS, Inc.
235 DeSiard Street
Monroe, LA 71201
800.729.2467
www.aims@aims1.com

1. Quantifiable impacts, by time:
 - a. Lost sales / revenue (e.g., lost new business)
 - b. Lost production (e.g., impact from failing to successfully deliver service)
 - c. Delayed revenue (e.g., cash flow)
 - d. Additional operating costs (e.g., overtime, additional costs)
 - e. Key internal operational statistics (i.e., transaction volumes)
2. Non-quantifiable impacts or consequences:
 - a. Impact on regulatory and reporting requirements
 - b. Intangible impacts such as customer service, image, investor confidence, and reputation
 - c. Employee and societal health and safety consequences (e.g., environmental, employee morale, indirect community financial impacts)
 - d. Operational impact (e.g., workflow)
3. Continuity preparedness and exposures identified during the data gathering process, including the data center/equipment and business units, noting such capabilities and exposures as:
 - a. Operational contingency capabilities (e.g., manual fallback capabilities)
 - b. Existing alternate processing options (e.g., dispersed operating capabilities)
 - c. General level of preparedness (e.g., records protection program, departmental computer data backup and off-site rotation, etc.)
4. Other recommendations and observations