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/po 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-hot site 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
## Priority Applications/Servers

List the priority applications/servers that drive your business, the most critical periods when these applications are required and access the overall impact to your company if you cannot perform these functions.

Two key elements that must be considered within any disaster recovery plan are the:
- Recovery Time Objective (RTO), the acceptable amount of time required to recover the business function after an outage, in laymen’s terms, how long can you be down without these applications running?
- Recovery Point Objective (RPO), the time allowed to elapse since the last backup of your data prior to the outage, in laymen’s terms, how much data can you afford to lose?

(Examples include accounting software, email communications, website, payroll, etc.)

<table>
<thead>
<tr>
<th>Applications</th>
<th>Critical Periods</th>
<th>RPO</th>
<th>RTO</th>
<th>Server</th>
<th>Impact on Business – None, Low, Medium, High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: email</td>
<td>Daily</td>
<td>1 day</td>
<td>1 day</td>
<td>Email</td>
<td>High</td>
</tr>
<tr>
<td>Example: Payroll</td>
<td>15th and 30th</td>
<td>7 days</td>
<td>7 days</td>
<td>Desktop 1</td>
<td>Low – can cut manual checks temporarily</td>
</tr>
</tbody>
</table>
Backup Details
For some companies, it is easier to list servers and personal computers because multiple applications reside on each.

It is recommended that all critical server and critical personal computer data be backed up. Copies of the personal computer files can be uploaded to a server just before a complete save of the system is done. Personal computer backups are then saved with the normal system save procedure. This provides for a more secure backup of personal computer-related systems where a local area disaster could wipe out important personal computer systems. Are there Excel spreadsheets, etc on personal computers that are critical to your business? Personal computers can also be backed up by other solutions.

Copy the key applications that you listed in the previous section and fill in the rest of the details.

<table>
<thead>
<tr>
<th>Priority Applications</th>
<th>Storage Location</th>
<th>Amount of Data – MG/GIGS</th>
<th>Name, Type of Device</th>
<th>Storage Media</th>
<th>Approximate Restoration time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What Is Your Cost of Downtime?

Productivity
- Number of employees impacted
  X hours out X
  burdened hourly rate

Revenue
- Direct loss
- Compensatory payments
- Lost future revenue
- Billing losses
- Investment losses

Damaged Reputation
- Customers
- Suppliers
- Financial markets
- Banks
- Business partners

Other Expenses
Temporary employees, equipment rental, overtime costs, extra shipping costs, travel expenses...

Financial Performance
- Revenue recognition
- Cash flow
- Lost discounts (A/P)
- Payment guarantees
- Credit rating
- Stock price

Know your downtime costs per hour, day, two days...
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