**Part 4: BIA & BCP**

**Health Network Inc. New Risk Assessment Plan**

**By: Kaleb Alstott**

**Introduction**

A BIA is a study used to identify the impact that can result from disruptions in the business. The main goal of a BIA is the focus on the failure of one or more critical IT functions. A BCP is a plan designed to help an organization continue to operate during and after a disruption. The main goal of BCP is to be prepared for disasters or events that might occur and be able to recovery from said disasters.

**BIA**

**Critical Business Functions**

According to bcmpedia.org a critical business function is “business activities and processes that must be restored in the event of a disruption to ensure the ability to protect the organization's assets, meet organizational needs, and satisfy regulations.” In order to pinpoint the critical business functions, we need to set a scope for this project. Our scope has been defined to the data center. When looking at Health Network Inc, we will be focusing on the data center and its critical business functions.

* Servers
* Networking equipment, such as routers or switches
* Security, such as firewalls
* Storage, such as storage area network (SAN) or backup/tape storage
* Data center management software/applications

**Critical Resources**

Once we have defined the possible critical business functions it is our job next to identify the possible critical resources. A critical resource is the resources that are needed in order to process and run the possible CBFs.

* Internet access
* Cloud/backup storage
* Network connectivity
* Database servers
* Desktop Computer

**Maximum Acceptable Outage (MAO) and Impact**

A maximum acceptable outage (MAO) is the total amount of time the system owner is willing to allow for a business process outage, that also includes the possible impacts that may happen. The importance of a MAO is that it helps to determine which CBFs need to be recovered and restarted as soon as possible after a disaster, identifies the specific resources needed to restart the CBF, and helps to determine how soon these systems need to be recovered. The impact aspect of an MAO is mostly a ranking or a grade not necessarily the true exact impact it will have on the company.

|  |  |  |
| --- | --- | --- |
| **CBFs** | **MAO** | **Impact Level**  **(Low, Medium, High)** |
| Servers | 24 Hours | High |
| Network Equipment (routers/switches) | 24 Hours | Medium |
| Firewalls | 48 Hours | High |
| SAN/cloud storage | 72 Hours | Low |
| Data center applications | 48 Hours | Low |

**Recovery point objective (RPO) and Recovery Time Objective (RTO)**

Recovery time objective (RTO) is the time in which the system or function must be   
recovered, this applies to the systems or functions. Recovery point objective (RPO) is the maximum amount of data loss an organization can accept. This only applies to data and addresses the data that is being stored in databases and servers. This is a key step in finding out the possible mission critical business functions. The difference between an RTO and RPO is that RPO is not considered part of the MAO. Instead, the RPO is like a factor or contribution about how much data loss and cost the business process can tolerate during the recovery process.

|  |  |
| --- | --- |
| **Systems/Functions** | **Recovery Time Objective (RTO)** |
| Internet Access | 8 hours |
| Desktop Computers | 4 Hours |
| Database Servers | 12 Hours |
| Backups/storage | 24 Hours |
| Network Connectivity | 12 Hours |
| Applications | 8 Hours |

RPO is a very hard concept to grasp when dealing with possible data loss for a company. When looking at Health Network Inc, we are a health care business that deals with customer information and customer transactions. Our database server is going to be the highest of importance due to the data and information it holds with our customers. Being down for half a day could be absolutely devastating depending on when our last backup was. Our RPO ideally would be no less than 8 hours and even then, we are missing out on tremendous of data for our customers and their health.

**Business Continuity Plan (BCP)**

A business continuity plan (BCP) is a plan designed to help an organization continue to operate during and after a disruption. The importance of a BCP is that it ensures that the organization is better prepared for disasters. After we have defined all CBF, critical resources, equipment, data, supplies, and documents like we have above we can move onto the four key phases of the BCP which are the notification/activation phase, recovery phase, reconstruction phase, and lastly forming a plan training, testing, and exercises phase. It has come to my attention that there is a specific request wanted in the BCP which we will touch on such as winter storms on the East Coast affecting the ability of Health Network employees to reach the Arlington offices in a safe and timely manner.

**Notification/Activation Phase**

One of the key parts to the BCP is the start and how we notify and activate the BCP, simply the BCP coordinator declares the notification and activation phase, which is when   
the disruption has occurred or is imminent. Once notified there will be a team in place to assess the damage of the equipment and/or company, this team will be known as the damage assessment team (DAT). The main goal here is to identify the possible damage as quickly as possible a report back to the BCP coordinator to plan out the activation phase.

Once the damage is reported, we move on to the activation phase. In this phase we start to activate the BCP accordingly from what our DAT found. Depending on who or what is damaged or will have an effect from said disaster we will need possible personal location control from, and possibly an alternate assessment procedure, all depending on what the DAT was able to find and assess.

For an example, with our conflict of the snowstorm, we first would start by identifying the possibility of employees coming in still and what the risk of the employees coming in would be compared to working remote. Once the risk and DAT have identified the possibilities, we would then start to implement a change in plans and activate certain BCP protocol.

**Recovery Phase**

In this phase of the operation is when we get down to the true nit and grit of fixing the disaster that has occurred. In this phase we send out our tactical response team (TRT) with the main goals of restoring temporary operations to the critical systems at sake, repairing damage done to the original systems, and recovering damage to original systems. It is key to understand that the TRT does not focus on recovering and restoring all operations, but instead focuses only on the CBFs that are identified in the BIA above. The success of this phase depends on four key components which are recovery planning, recovery goal, technical recovery team lead, and lastly technical recovery team. For our example of the possible weather storm, if employees weren’t able to come in our TRT would simply set up VPNs and possibly set up connectivity to employers.

**Reconstruction Phase**

In the reconstruction phase we focus on both the critical and noncritical functions that are being returned to normal. To begin this phase, we would start off with the damage of the original location being repaired, and/or possible management decision to move operations permanently to an alternate location if need be due to left over possible risk. If there is possible damage from the original site, management could possibly move operations to a different location. Lastly, once we have declared, if possible, damage is recovered or moved to an alternate site it is time to plan a slow and steady deactivation of the TRT. In our case with the example of the winter storm, once the storm is passed and possible employees can return to normal work, it would be advised to slowly remove the TRT off the VPNs and connectivity to the employees form at home locations.

**Plan Training, Testing, and Exercising**

Lastly, in this phase of the operation we have ultimately recovered from disaster and this phase would typically take place before a disaster would occur. To start off, all BCP need to be tested to find possible flaws or loops in the system. In this step we would set up exercises to test out our possible plan. A possible exercise that we could implement is possibly having employers work from home for a day to test our systems and how we would possibly hold up if a snowstorm were to happen. We have three main goals in this step which are

* Training—Teaching people details about the BCP
* Testing—Verifying that the BCP will work as planned
* Exercises—Demonstrating how the BCP will work

We have covered how we will test and what type of exercises we would do to be prepared for our BCP but lastly, we need to touch on the training for the BCP. Our training would look like how you would connect from an at home work station, when to stay home vs. come into work, how to connect to the companies VPN, and overall preparation for what to come.

**References**

MRIS-3E-Chapter13.pptx

MRIS-3E-Chapter12.pptx

<https://www.bcmpedia.org/wiki/Critical_Business_Functions_(CBF)>

<https://www.sciencedirect.com/topics/computer-science/critical-business-function>