Bellevue University

Eric Wellmaker

M10 Writing Assignment

Physical, Oper & Personnel Sec

February 18th, 2023

In the event of a natural disaster or security breach, contingency planning or “backup planning” can be thought of as a roadmap or guide to restore services after an anomaly has transpired. This instructional guide will help a business restore its services in the most efficient manner possible. For this discussion, I will explain in detail what contingency planning is and why it is necessary. I will also explain the subordinate functions and the relationships between BIA (Business Impact Analysis), IRP (Incident Response Plan), DRP (Disaster Recovery Plan), and BCP (Business Continuity Plan). And in the final section I will provide an example of a resource page that can be used for contingency planning.

Contingency Planning and Introduction of subordinate functions

Contingency planning is a “Plan B” or backup plan that is designed to help a business, company, organization, etc. react to an unplanned future event that would damage or destroy products, goods, or services. Contingency plans are not set in stone, instead they are designed for situations with the likelihood of coming true (Kirvan, P., 2023). The subordinate function of a contingency plan further breaks down what should be done to recover from an unseen event. The first subordinate function is the BIA (Business Impact Analysis). It is here that a prediction is formulated to determine the severity of a business and its functions if they were stopped. The BIA also acquires data so the organization can devise a recovery plan (Business Impact Analysis., 2021). IRP (Incident Response Plan) clarifies the roles and responsibilities of assigned personnel during a confirmed or suspected security incident. DRP (Disaster Recovery Plan) devises a baseline standard for recovery in the event of major disruption of services, goods, or products. While disasters are rare, (earthquakes, tornadoes, tsunamis, etc.)

it's imperative to have a response plan in place to refer to, in the event outages are reported (Disaster Recovery Plan Policy.,2014). The BCP (Business Continuity Plan) is necessary when a business cannot operate as its intended. The BCP is a step-by-step guide for initiating recovery steps after a disaster, or negative anomaly has transpired. These subordinate instructions that were covered will provide all the necessary information for a business to return to normal operations. In the next section, I will go into further detail about the four subordinate functions and explain their relationship to each other.

BIA, IRP, DRP and BCP

For this section, it would be easier to describe the four subordinate functions using them in an example where a business has suffered from a disruption of an electrical power loss. Business "A" had an assessment made to determine the effects of a disruption from its goods and services. The BIA identified that a scenario like losing electrical power would reduce utility productivity, damage to machinery and equipment and personnel being unable to access some restricted areas due to there not being sufficient power being supplied (Business Impact Analysis., 2021). Next after the BIA was to review the IRP (Incident Response Plan) to determine who Business "A" should be calling and why. And, to also identify key personnel to restore services (Incident Response Plan (IRP) Basics.,2021). There should also be an Incident Manager to lead the response for Business "A" and communicate with various agencies, prioritize what needs to be done and log what events lead up to the stoppage and why so the disruption will not be repeated in the future (Incident Response Plan (IRP) Basics.,2021).

After the Incident Manager gathered enough data, it was discovered that there was some flooding by their main facility. More so, the generators for Business “A” were partly submerged and were inactive. Gathering the DRP (Disaster Recovery Plan), the manager started to identify requirements to return Business “A” to an operational condition. Since this was an electrical power outage, there must be a determination if company data was backed up, lost, or has capability of being restored. As a safe measure, the DRP should be reviewed annually to ensure guidelines, contact numbers and response providers are all current (Disaster Recovery Plan Policy. (2014). Next the manager reads the BCP (Business Continuity Plan). It is here that a strategy will be laid out to restore Business “A” to normal operations. The BCP will include a risk assessment threshold where it can be determined the minimum required necessities to get Business “A” back to operations. These necessities will include utilities, vital records, employees, third party services, costs and resources. Time is always a factor so when planning for restoration of services, a grace period should be given for services to arrive and the time needed to return to normal operations (Business Continuity Plan., 2021). For the final section, I will provide an example of a contingency resource page.

Contingencies Resource Page.

Contingency Plan

Version: 1.00

Version Date: 02/19/2023

Version Number	Implemented By	Revision Date	Approved By	Approval Date	Changes
1.00	Eric Wellmaker	02/19/2023	Eric Wellmaker	02/19/2023	None

This template is an example of the necessary steps taken to mitigate an incident. The contingency plan lays out a road map on what to do and who to call to restore a business to baseline operating functions. The plan will be divided into three sections: Identification of event, Mitigation & restoration, and restoring a business to normal operations (EPLC Contingency Plan Template., 2022).

Identification of event 1.1.

1.1.2 For Security Breach in IT call <xxx-xxx-xxxx> and ask for <Name>

1.1.3 For fire call <xxx-xxx-xxxx> and ask for <Name>

1.1.4 For earthquakes call <xxx-xxx-xxxx> and ask for <Name>

1.1.5 For floods call <xxx-xxx-xxxx> and ask for <Name>

These offices are available 24/7 and will have a provided checklist for procedures needed to mitigate actions above.

Mitigation and restoration 2.1.

2.1.1 Talk to dispatch agent and provide information on how security breach was discovered, time, and location.

2.2.2 While on the phone with dispatch, give a description about the fire if possible: Class A, B, C, D, K. Provide information if an attempt was made to extinguish fire. Any personnel injured? Building or equipment damages?

2.2.3 While on the phone with dispatch, give time and duration of earthquake. Number of injured personnel and damage assessment.

2.2.4 While on the phone with dispatch, give information about flooding, location, equipment damaged, and personnel injured (if any).

The member will give as much information as possible so dispatch can give the correct number of resources to the location that needs assistance.

Restoring a Business to normal operations 3.1

3.1.1 Member will follow recommendation from IT dispatch to mitigate security threat. Log incident and perform advised upgrades to prevent future security breaches.

3.2.2. Member will follow guidance from fire response dispatch.

3.2.3. Member will follow guidance from emergency response after the earthquake has happened. Member will give detailed damage assessment so emergency dispatch can notify other agencies if needed.

3.2.4 Member will follow guidance for flood mitigation procedures.

Events leading to and mitigation techniques will be documented to determine the effectiveness of the contingency plan. Changes will be warranted with any updates to resources or more stream-line approach to negative trending events (Incident Response Plan Example., n.d.).

Contingency planning is necessary for a business to return to normal operating parameters after a negative event has transpired. BIA, IRP, DRP and BCP all list guidelines for a business to follow, and resources to contact to ensure a smooth transition from a workflow stoppage to a restart of goods and services. With proper preparation, contingency planning can help a business learn from its mistakes and recover from a work stoppage.

References

Business Continuity Plan. (2021). Ready. https://www.ready.gov/business-continuity-plan

Business Impact Analysis. (2021). Ready. https://www.ready.gov/business-impact-analysis

Disaster Recovery Plan Policy. (2014). SANS. https://content.bellevue.edu/cst/cybr/510/Documents/disaster_recovery_plan_policy.pdf

EPLC Contingency Plan Template. (2022). Officeapps.live.com. https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.hhs.gov%2Fsites%2Fdefault%2Ffiles%2Focio%2Feplc%2FEPLC%2520Archive%2520Documents%2F36-Contingency-Disaster%2520Recovery%2520Plan%2Feplc_contingency_plan_template.doc&wdOrigin=BROWSELINK

Incident Response Plan Example. (n.d.). Bellevue University. https://content.bellevue.edu/cst/cybr/510/Documents/Incident%20Response%20Plan%20Example.pdf

Incident Response Plan (IRP) Basics. (2021). Cisa.gov. https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

Kirvan, P. (2023). Contingency Plan. TechTarget.

https://www.techtarget.com/whatis/definition/contingency-plan