OPEN ACCESS Freely available online

Journal of Information Technology & Software Engineering

Research Article

IT Infrastructure - Business Continuity Plan Implementation and Maintenance

Anshuman Awasthi *

Department of Engineering, Restoration Hardware, USA

ABSTRACT

Business Continuity Planning requires many efforts from cross-functional team members across the organization. If creating a plan is such a big commitment, maintaining and regular, testing requires even more dedication towards the initiative. Many organizations invest a lot in creating a plan and documenting the process but sometimes fail to keep the plan active overtime. Let us review the complex exercise of maintaining and exercising Business Continuity Plan implementation from an IT Infrastructure perspective.

Keywords: Business; Continuity; Planning; Risk Management; Risk Mitigation; IT Infrastructure Risk Factors; Business Continuity Implementation

PROBLEM DEFINITION

How to execute and maintain an effective Business Continuity Plan.

DISCUSSION

This article explains how to start working on the prerequisites of a Business Continuity Plan and implement the same. It also explains some of the aspects of maintaining the plan and how to communicate during the crisis.

METHODS

Business Continuity Planning; Risk Management

INTRODUCTION

If we need to prepare our organizations' critical business functions against any disaster, it is essential to invest in a robust Business Continuity Plan. This initiative requires a lot of preparedness before we can start documenting the process. Let us review some of the major prerequisites.

Regular Backups and data stored at offsite location: If we schedule regular backups in the cloud or at least to an external hard drive, it is a quick method to ensure that all your data is stored safely. It is essential to have a backup policy in place. Servers should have a full back up at least every week and incremental backups every night; we also need to backup personal computers completely every week, but users can do incremental backups every few days [1].

Employee education and training

Teaching all our staff about proactive defense and safe online habits is critical.

"Educating them about what they are doing and why it is dangerous is a more effective strategy than expecting your IT security staff to react to end-users' bad decisions constantly," Watchinski says [2]. The company needs to ensure that all employees understand how important our company's data is and how to ensure data safety in case of a disaster and during normal operations.

Risk Register

The organizations can prepare a risk register based on their corporate /branch office/ Date Center locations, critical business functions. Please refer below example of a sample risk register for an organization.

Name of Risk	Description	Source (with explanation)	Likelihood of Occurrence* (with justification)	Severity of Impact* (with justification)	Controllability* (with justification)

*Correspondence to: Anshuman Awasthi, Director-Department of Engineering, Restoration Hardware, USA, Tel: 8187514274; E-mail: anshumanawasti@gmail.com

Received: February 15, 2021; **Accepted:** March 1, 2021; **Published:** March 20, 2021

Citation: Awasthi A (2021) Enterprise Network Hardware Refresh. J Inform Tech Softw Eng. 11:253.

Earthquake	Company's headquarters are located near San Andreas fault line and an earthquake can cause damage to corporate office and data center	External-Earthquake is one of the natural disaster	Medium-Company headquarters are not inside San Andrews fault line but near to the area	High-Earthquake can cause severe and disruption	Low-We cannot control earthquake but just prepare for business continuity
Internet Services	Internet services outage from a provider will cause service disruption as site operations depends heavily on internet connectivity	External-Internet connectivity is provided by internet service provider(ISP) on their own network	Medium-We have chosen a well-known (ISP) with reliable network infrastructure.	High-Internet outage at a critical site can cause severe impact to operations as important resources are available on network	High-It can be controlled by agreeing on aggressive SLAs with ISPs and installed network circuits from multiple vendors
Power Outages	At a facility or across a power grid	External-Power is provided by external companies	Low-Power outages are not common in area	High-We depend heavily on network and IT resources to run operations which will need power to function	Medium-It can be controlled by use of uninterruptible power supply(UPS) and generators
Hardware Failures	Due to normal wear and tear, facility damage, or human error	Internal-Hardware failures in network equipment's, servers and storage are common and can happen due to normal wear and tear	Low-We have installed hardware supplied by a well-known vendor and they guarantee their performance	Medium-Impact can be minimized by running servers in high availability environment	Medium-We have installed redundant servers for all critical applications
Fire/Heat Damage	Whether from equipment overheating, short-circuit, lightning, loss of environmental controls, or arson	External/Internal-Overheating of any network equipment or fire originated from an external source can cause damage.	Low-Company is taking precautionary measures to avoid overheating of equipment's and is performing regular fire-drills	High-Fire/overheating can cause significant damage to critical hardware equipment's and will directly impact operations	Low-Fire can be controlled by having fire extinguishers onsite and an immediate call to fire department
Water Damage	Whether from leaky pipes/roofs or severe weather	External/Internal-Water damage can happen from internal pipes or from external factors like severe weather	Medium-We carryout regular inspection of plumbing infrastructure and drainage system to avoid occurrence	High-Water damage can cause severe damage to company property disrupt company operations and can cause loss of revenue	Low-Water damage due to internal factors can be controlled but we have very limited control on water damage caused by external factors.
Product Supply	Companies makes profit on sold products. If there is any impact to the product supply it directly affects companies business and reputation	External-Vendors located in different countries manufacture most of the products overseas. Vendor financial stability ,political unrest in their home country will affect product supply	Medium-Company had varies vendors located in different countries	High-Supply chain is a critical function of a retail organization and any disruption in product supply will have direct effect on revenues	Medium-Company has a very limited control on external factors effecting product suppliers in different countries

Table 1: Risk register.

DISRUPTION SECURITY MEASURES

The Basic System Security Measures should apply to all systems at an organizational level, regardless of the level of their system type. It is a critical baseline, which all systems must meet. Please

refer to below security measures, which can be applied even in case of a disaster.

Accountability and audit

Enable process accounting or auditing: Enable process accounting or auditing that can generate an information log about how the new processes are created and their log activity.

Audit change in privilege or privilege escalation: Whenever a user changes his level of privilege, a log should be generated to record that.

Audit firewall denial: When the host or a zone-based firewall denies any network communication system should generate a log.

Audit all critical application events: It is essential to log all critical application events.

Dedicated Syslog system: System logs must be written to a remote system in such a way that any user on the system being logged cannot alter them [3].

Configuration and maintenance

Follow advanced vendor security recommendations: Conform to guidance and best practices as per the vendor's security documentation and whitepapers.

Network-based firewalls and Host-based: Systems must be protected by both a network-based and a host-based -firewall that allows only those limited incoming network connections required to fulfill the business need.

Change management process: Configuration changes must be regulated by a documented change and configuration management process.

Partitioning: Systems may share resources and hardware only with other systems that have similar security requirements, regardless of their criticality classification. Systems that share the same security requirements have user communities of similar size and character, identical firewall profiles, and same technical specifications [4].

Access control: No system or person should be given access to the critical systems unless it is required for business purposes.

Sharing: Critical data will not be shared with any unauthorized application. If an application needs access to data that requests need to be approved by change advisory board

Retention: Critical data should only be stored for as long as is necessary to accomplish the documented business process [5].

Physical access:

The system must reside in a secured, managed data-center.

COMMUNICATION PLAN

It can be very challenging to communicate during a major disaster. It can be almost impossible, as thousands of people attempt to reach families and friends and to ensure their safety or inform on their situation [6]. Cellular communications are often considered the most reliable during weather or power emergency, and the vast call volume can cause strain on the mobile network, making calls difficult [7].

To overcome this obstacle, an organization's crisis communication plan should include various methods to reach its key stakeholders, such as:

- Emails, text messaging,
- Social media outlets (Facebook, Twitter, LinkedIn, etc.),
- A business telephone hotline with recorded messages with the capability of allowing the caller to leave voice messages,
- Intranet site or a business' website or a third-party emergency notification system.

An organization needs to understand that a business' crisis communication goal should be to provide accurate, timely, and precise information to prevent inaccuracies and rumors. If we want to accomplish this objective, our BCP communication should include a message containing the following verified information that will be sent to all stakeholders as soon as possible after a disruption has occurred:

- When what, and where disruption has occurred
- How critical the problem appears as of now
- How the business operations have been impacted (e.g., damage to operations and facilities)

Additional information should be sent to employees, including:

- Who is expected to report to work
- Where and when to report to work
- Where to direct questions
- When more details will be available

All communications will be tailored to the recipient, considering what they may experience because of the disaster. It helps to maintain the business's good reputation, and it also provides practical information regarding where and when the business will be "open for business."

The company can use a template as the one shared below to send a message to its employees:

PREPARED MESSAGE TO EMPLOYEES
[Template]

First notice

A severe storm has developed over [area] and is estimated to continue through [time] am/pm. Please relay this information to all affected individuals in your department/work area, including any onsite visitors.

Notice of delayed opening

Due to the current weather conditions, the ~ corporate office will have a delayed opening on [date]. The office will open at [time] am/pm. Please call [contact name/phone] or check the website www.organizationwebsite.com to verify the status of the office prior to your commute.

Notice of closure

The [business name] will be closed [date] due to the severe storm. Those employees who are expected to report to work will be notified. It is anticipated that the [business name] will reopen [date], depending on conditions. As more information is available, we will contact you by [phone/email/text] by [time] am/pm. Please call [phone] or check the website [URL] to verify the status of the office prior to your commute. Optional: Employees who were scheduled for work today will receive their regular full day wages according to their normal work schedule.

Notice of re-opening

The corporate office will reopen [date]. Those scheduled to work are expected to report to work at their designated starting time. However, we do not expect any employee to take unreasonable risks attempting to report for work. Each employee must observe conditions in his/her own area and determine whether aftermath conditions or circumstances will make the trip unduly hazardous. You must notify your supervisor as soon as possible, if you will be unable to report to work or if you will arrive late [8]

Stakeholder communications

Information management and communication should be a part of planned design and execution and should be integral to the organization's risk and disaster management plans. The improvised conversations can be costly and have unsatisfactory results.

During an emergency, timely and transparent production and dissemination of information generate trust and credibility [9]. All stakeholders involved will demand information in the form of data, figures, reports, and situation analysis or recommendations. These stakeholders depend on this information to guide their work and to translate their interest and concern into concrete action.

The company can use a call tree to communicate with all stakeholders. A call tree is a layered structured communication model that can be used to notify defines individuals in case of an event ~ typically unplanned ~ and coordinate the process of recovery if required. A call tree is also referred to as a phone tree, call list, phone chain, or text chain [10].

The organization's IT and business functions can create their call tree coordinates data gathering with their HR (Human Resources), as contact data typically comes from that department usually. Each listed staff may have several contacts, including home, office, and cell phone numbers, and an email address. The emergency management team and company management then approve the list of contacts, and sequence of notification. The emergency call tree is available in several locations-such as the company intranet and in hard-copy format.

Call trees play an essential role in our disaster recovery plan. Call tree execution should be automated with the help of any application and that software can contact all stakeholders using a landline, email, cellphone, text message, or another type of listed communication in the process.

In case of an incident, the call tree is initiated once the Disaster Recovery team has completed their assessment and determined that employees must be notified. Only designated employees can launch the emergency call tree once it approved by an authorized leader.

As the call tree progresses, incident response team members take notes on people they cannot contact, as the data must be conveyed back to the Disaster Recovery team for further follow-up. To ensure calls were completed as planned, the last person on the call tree list should confirm receipt of the final call to an employee. The company also has a communication list manager to monitor responses and contact backup staff as necessary.

Once the entire call tree has been notified, other business continuity plan procedures can proceed. Call tree benefits include human interaction, the ability to relay important information, and the creation of a comprehensive list of stakeholder's contact information.

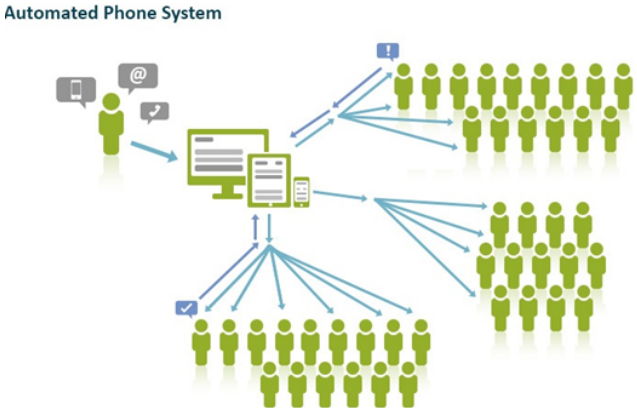

Figure 1: Call Tree.

During an incident, the call tree is initiated once the emergency management team has completed its assessment and determined that employees must be notified. Only designated employee can launch the emergency call tree once it approved by authorized leader. As the call tree progresses, incident response team members take notes on people they cannot reach, as that data must be relayed back to the emergency team for follow-up.

To ensure calls were completed as planned, the last person on the list should confirm receipt of the final call to a designated employee. Company also has a communication list manager to monitor responses and contact backup staff as necessary. Once the entire call tree has been notified, other business continuity plan procedures can proceed. Call tree benefits include human interaction, the ability to relay important information and the creation of a comprehensive list of stakeholder's contact information [11].

The company can follow below communication methods beyond automated call tree procedure

- Conference calls
- Person-to-person communication
- Website notification

- Dedicated Message center
- Customer notification
- Progress reporting
- Employee reporting
- Text-to-speech messaging

RESTORATION OF OPERATIONS

If an office facility is damaged or production equipment breaks down, information technology is disrupted, business is impacted, or a supplier fails to deliver or and the financial losses are beginning to increase. The organization recovery plans are alternate means to restore critical business operations to a minimum level that can be acceptable following a business disruption, and they can be prioritized by the Recovery Time Objectives (RTO) decide during the BIA (Business Impact Analysis).

Recovery strategies require resources, including facilities, people, and equipment, materials, and information technology.

Company Operations can be relocated to its alternate site in a different city in case of any disaster affecting their primary location - assuming the same outage does not affect both. This method also believes that the surviving site has the capacity and resources to perform the allocated work of the site that is affected. Prioritization of service levels or production, providing additional support and staff, and other action items that would be needed in case of capacity issues at the other site. Company staff can work from home through remote connectivity [12].

The organization should identify its critical applications, and they are categorized into two sections;

a) Applications met strategic guidelines; Applications that are having Development and QA environment on a designated alternate location other than production [13].

b) Apps do not meet strategic guidelines; Applications that are having Production, Development, and QA environment in the same Data Centre (DC) [14].

DR Solution Strategy High Level Overview of identified business critical applications

Applications Environment Meeting Business Strategy	
Applications having Production in Primary DC or Secondary DC and corresponding Dev/QA environment in alternate location-Primary for Secondary DC and vice-versa	
Applications	**Strategy**
SAP Financial	**Replication Solution:** VTL Based Replication/Oracle Data Guard
System Enterprise Services (ESS)	**Compute:** Existing Dev/QA environment will be utilized
Oracle AR	**Core Infrastructure & Application:** Existing Infrastructure will be leveraged
Word Financials	**RPO and RTO:**4 Hrs< RPO< 24 Hrs and RTO 48 Hrs
Email & Black Berry (Independent apps no Dev/QA)	**(Note:** Email/Black Berry no data would be replicated from production environment, only identified VVIP users mailbox will be created at alternate recovery site during the Disaster Situation)

Table 2: Application Strategy 1.

Applications Environment Not Meeting Business Strategy	
Application having Production environment in Primary and Dev/QA environment in alternate location-Primary or any other site (other than Primary Location)	
Applications	**Strategy**
Atlantic Royalties	Replication Solution: Tape Based Replication Solution
	Compute: Existing Dev/QA environment will be utilized
WBR Royalties	Core Infrastructure & Application: Existing Infrastructure will be leveraged
SMART	RPO and RTO:24 Hrs< RPO < 48 Hrs and RTO 48 Hrs
Applications having Production and Dev/QA environment in same location	
Applications	**Strategy**
Core Financials	Replication Solution: Tape Based Replication Solution
	Compute: Back-to-Back Agreement with the Third Party Vendor to supply required compute resources within agreed SLA's.
	Core Infrastructure & Application: Existing Infrastructure will be leveraged
	RPO and RTO:24 Hrs< RPO < 48 Hrs and 24 Hrs< RTO < 120 Hrs

Table 3: Application Strategy 2.

An example of an Organization's disaster recovery solution strategy

Compute: Development/QA environment compute resources would be utilized during the disaster situation. Existing Dev/QA

operating system instances would be required to shutdown with necessary precautions before recovery of the production environment on identified servers [15].

Operating system: Recovery location side operating system can be kept in sync with the production environment using VTL based replication.

Database: The production environment would be required to configure as Primary Database with archive mode on. Recovery location Database would need to be configured as a standby database, and Archives logs would be shipped to a remote location at regular frequency using automated scripts/Oracle Data Guard. These archive logs would be applied at regular intervals to sync up the standby database with the primary database.

File system: Any file system, which is required to be available at recovery location need to be replicated using VTL based replication.

Core infrastructure: Active Directory & DNS can serve from an alternate location in case of any disaster declared [16]. Citrix environment is running as a single Citrix Farm with multiple zones that are serving respective areas; client application software that is installed and published using Citrix would need to be installed and released from another zone.

Network infrastructure: Core network infrastructure is already established in Primary and Secondary DC's, System ESS uses the same resources for user access. Internal stores network users are considered as trusted user's equivalent to Local Area Network (LAN) users, so there is no firewall for Stores environment. The organizations Virtual Private Network (VPN) users that are accessing this application through SecondaryVPN, in case of unavailability of primary VPN, users can select alternate available VPN servers to connect to the organization's private network.

User redirection: All users will be redirected to the Recovery location automatically. During the disaster situation, the Citrix/AD/DNS environment of New Jersey location will redirect the end users' requests to the secondary System enterprise services environment [17].

Oracle AR: The Standalone Oracle AR module is implemented mainly as a cash application. There are a high number of custom forms and functions registered in Oracle AR. The Descriptive Flex Fields (DFF), Standard flex fields available with Oracle are also used to capture data such as information coming from Legacy systems, Collector Information, Custom Notes, etc. that needs to flow to the downstream systems and also from the data that needs to flow from other systems to Oracle. Reconciliation and reporting are carried out using customized reports that generally are run during month-end for checks and reconciliation. These are mainly aging reports and customer balance reports.

Let us say that the organization's staff logs in to Oracle Applications through the E-Business Suite Home Page that is accessible using a desktop client web browser. The user interface is provided in two ways, either through HTML for the newer HTML-based JSP applications or through a Java applet in a Web browser for the traditional Forms-based interface.

Word financials: Word Entertainment is a data store of outdoor furnishing. The WORD system has been set up mainly for the Order-To-Cash functionality. The application can be accessed through a user interface, which is provided in two ways: HyperText Markup Language (HTML) for the newer HTML-based (Java Script)JSP applications or through a Java applet in a Web browser for the old Forms-based interface [18].

Word Financials interfaces with various application systems, like EDI-Gentrans, Oracle AR, Diamond, WEA, Etrans, Warehouse System, and SAP. Word Financials environment uses tools like Toad and/or SQL Navigator and Go Global-to connect to UNIX.

IMPLEMENTATION OF THE BCP

We can assume that catastrophic events may have a minimal probability, the organizations that plan carefully for their business continuity are the ones that may stand the best chance of continuing their essential business functions in case of a disaster. It does not take a monumental disaster to disrupt the daily operations of a business. Occasionally it can occur due to a power outage or intermediate interruptions that result from an attack instigated by cybercriminals or from a storm [19]

The organization needs to understand that having a Disaster Recovery Plan in place means arranging to continue to deliver essential services that are required to run business operations and identifying the necessary resources, which are vital to support business continuity. If we want our business continuity plan to be effective, the leadership team needs to work on below key critical components that must be present during the planning process.

Business continuity planning organization

When an organization starts the process of BCP, a senior management team is required to oversee the whole process, which includes initiating the necessary steps, designating the resources, planning for implementation, and then continue auditing and testing the business continuity plan[18]. The senior management committee creates the teams required responsible for developing and executing the business continuity plan, will approve the planning structure, identifies the roles of specific individuals, and prioritizes critical business operations.

Business impact analysis

By performing a Business Impact Analysis, an organization can identify essential business functions on both the external and internal levels. The identification of these business functions initiates prioritization of services to ensure ongoing delivery and fast recovery following a disruption.

Business Impact Analysis should also include an assessment of the impact a disruption can have on the service delivery model and how long a business can survive without running mandatory business functions. It is also essential to identify the areas, which contribute the most to the revenue and then

prioritize those business functions to prevent loss of income following a disaster. We need to consider the shareholders and the consumers, and when we are doing the BIA (Business Impact Analysis) to assess the cost of intangible losses that can be caused by an outage.

Business continuity detailed response and recovery plan

Following the setup of a leadership committee and the completion of a Business Impact Analysis, a business continuity plan needs to be documented to explain in detail how essential business services will be offered during the period of service disruption. Each function that is considered critical to the business operations will be carefully planned in detail. It will include identification of all possible risks and threats, recovery processes that are already documented and communicated by the business, and appropriate response to the disaster by the respective teams that are knowledgeable in their area of service and in case we need to relocate to an alternate space.

Training

When the Disaster Recovery plan is in place, we understand it is critically necessary to train our workforce on their designated responsibilities in the event of a disruption. In addition to being trained on their specific duties, our workforce should also be aware of other cross-functional team functions that are associated with their responsibilities. The training will include several learning exercises that set the stage for the Business Continuity Plan and prepare our employees for the necessary actions they should take in the event. It should include the proper sequencing of tasks and what should be their response to any external factors that can have an impact on the overall recovery process.

Quality assurance

Following the training phase, the organization's recovery Team will evaluate the Disaster Recovery plan to find out where improvements are required and to assess the program for effectiveness and accuracy. This process is also referred to as quality assurance, and it will be performed both on the external and internal levels to ensure the efficacy in the event of disruption of services.

COMMUNICATION OF THE BCP

An organization should recognize the importance of crisis communication by encouraging practices to obtain and maintain vital contact information for their workforce, vendors, customers, to ensure communication systems will operate even if the business is closed. The key is hidden in knowing how and when to communicate essential information to keep those you rely on, and those who are dependent on you.

The organization's Business Continuity Planning team should understand that we have multiple stakeholders who should be included in a crisis communication plan. That said, the most critical and immediate targets are employees as to when the disaster happens, they need to know about damage to their workplace facilities like their branch or corporate office and the status of operations. The employees should be equipped with this baseline information, it is essential to reach out to others based on the nature of the issue the organization is facing (e.g length of likely closure damage to the building, financial needs, etc.). In a typical scenario, this should include critical suppliers, customers, neighboring businesses, utility companies, and creditors, as well as essential business partners such as financial institutions and insurance agents.

The enterprise should understand that for an organization crisis communication goal should be to provide accurate, timely, and correct information in a simple format to prevent inaccuracies and rumors. To accomplish this objective, our BCP communication should include a message containing the following verified information that will be sent to all stakeholders as soon as possible after a disruption has occurred:

The company can follow the below steps to communicate the Business Continuity plan to all stakeholders involved.

Assign a communications coordinator

The company should identify a crisis communication coordinator. This person will be responsible for communicating the business continuity plan and developing messaging, managing the communications process, and working with the business owner or other senior management on preparation and implementation.

Create message templates

The organization's business continuity planning team should prepare message templates with the information, which is relevant to the necessary stakeholders as per their role [20].

Create an employee emergency card

The organization should create and distribute a pocketsize emergency card or print the information at the back of the employee's identification card, which includes critical information that may be needed during or immediately after a disaster. Many organizations operate primarily as a paperless office. Still, they need to understand a small employee emergency card can be used as a useful resource (even by a few employees) that should be easy to access if electronic devices are down.

Use of all available mediums

The organization should schedule overview training, update the intranet website, and will inform all department heads to reach out to all the concerned individuals.

MONITORING AND TESTING OF THE BCP

An enterprise should understand that it is crucial to have a business continuity plan because in the event of an outage that causes a business shutdown–a fire or flood for example—the organization should be able to minimize losses, downtimes, and the impact on your customers. Once we have developed our business continuity plan (BCP), it is just as important to test the program. Testing verifies that the method is useful, it helps to

train all the participants and prepares them to perform in a real scenario and identifies areas where the plan needs to be strengthened.

The organization can include below activities to ensure they test the plan appropriately:

- Conduct a plan review at least quarterly. Gather our team of key Business Continuity Plan participants–division leaders or department heads–regularly to review the business continuity plan. Discuss various sections in the program with a focus on the discovery of any areas where the project can be strengthened. Train new managers regarding the method and incorporate any further feedback.
- Conduct disaster role-playing ("table-top") sessions that allow plan participants to "walk through" the facets of the BCP, gaining familiarity with their assigned responsibilities in the specific emergency scenario(s). It is essential to perform a dry-run training to document errors and identify inconsistencies for correction and improvements. Schedule at least two to three of these sessions each year.
- Perform a dry run of a possible outage scenario. Include business partners, leaders, vendors, management, and staff in the BCP test simulation. Test data recovery, staff safety, asset management, leadership response, relocation protocols, and loss recovery process. Plan a complete simulation testing at least once a year with realistic but different scenarios that test the effectiveness of our documented process.
- An organization should account for any work interruptions caused by the testing of the disaster recovery plan by scheduling simulations and other exercises like dry runs and limited testing, possibly on weekends. Conduct tabletop sessions that include higher-level staff and management exclusively between Saturdays-Sundays, and plan for all the review meetings usually lasting between two to four hours that can be scheduled during the regular working hours.
- Communicate the benefits and importance of the Business Continuity plan to all levels of the workforce. Promote the review and active participation in the BCP simulation. Use the simulation to identify competencies within our workforce that may signify additional resources during a disaster situation.

The organization should monitor all critical incidents by establishing an Incident Command System (ICS). The Incident Command System (ICS) is a modular incident management system designed for all hazards and levels of incident response [15]. This system creates a combination of facilities, equipment, personnel, procedures, and communications operating within a standardized organizational structure. The use of the Incident Command System at the organization facilitates the company's ability to communicate and coordinate response actions with other jurisdictions and external incident response agencies.

The primary responsibility for monitoring Incident threats and events resides with Incident Response teams and facilities. Incident response team serve on a continuous 24/7/365 basis and is always available to receive Incident communications from a variety of official and public sources, including National Warning System, National Weather Service (NWS), State Police, Fire, and Incident Medical Services Institute communication systems and Incident telephone calls [11]. The incident response team has a detailed checklist to follow during the incident to monitor if the business continuity plan is being executed as per the policy.

ADJUSTMENT OF THE BCP

The company should integrate business continuity planning into every business decision, incorporated plan maintenance in job descriptions, and has assigned responsibility for periodic review of the plan and perform regular audits and tests.

An organization can appoint as business recovery coordinator who will be responsible for ensuring that the BCP plan is up to date. The Recovery teams, in turn, are performing their responsibility of updating, reviewing, and different sections of the program and any associated related materials. The recovery management team is also responsible for the incident management procedures and overall plan coverage, making sure the plan addresses any new risks as changes to the company, and its operations take place

The organization should update the business quarterly and get the updates applied to the plan, and the revision history is updated to record the changes. To keep the plan current, an active program of testing or exercising is followed as listed below, and inputs received post review exercises help to keep the plan up to date.

- The company should conduct a plan review at least quarterly. Gather the team of key business continuity plan participants–division leaders or department heads–regularly to review the business continuity plan. Discuss the elements of the project with a focus on the discovery of any areas where the program can be strengthened. Train new managers regarding the policy and incorporate any further feedback.
- The company conducts disaster role-playing ("table-top") sessions that allow plan participants to "walk through" the facets of the BCP, gaining familiarity with their responsibilities given a specific emergency scenario(s). Conduct the dry-run training to document errors and identify inconsistencies for correction and improvements. Schedule at least two to three of these sessions each year.

COMMUNICATION OF CHANGES

The primary goal of (BCP) is to restore operations through predetermined, systematic processes and procedures efficiently. However, to minimize the impacts and rapidly respond to operational hindrances, companies must ensure business continuity communication methods and systems are clearly defined and functional. An organization should understand that the BCP plan update and its communication is an intricate part of any continuity process and the overall preparedness. Effective and transparent communication channels must remain available to assess and relay damage, disseminate information to employees, and coordinate a recovery process. Incomplete communication often results in failed business continuity efforts. Disaster Recovery ensures thorough planning, testing, and exercising communication procedures within the following,

four phases for effective business continuity and viability of critical business operations.

Notification: The notification process begins when relevant changes to the business continuity plan have been made. Appropriate personnel and applicable business unit managers are initially notified and updated on changes. The organization's communications policy can instruct the original notification format.

The person responsible for each critical business process starts updating related documents. Necessary continuity information needs to be maintained and updated as required to ensure all management and affected personnel can quickly initiate proper actions.

Plan review sessions: Disaster Recovery team conducts a plan review at least quarterly. We gather our team of key Business Continuity Plan participants--division leaders or department heads--regularly to review the business continuity plan. Discuss the elements of the project with a focus on the discovery of any areas where the program can be strengthened. Train new managers regarding the policy and incorporate any further feedback.

Verification: Verification of contact information for personnel, continuity supervisors, and external responders should be done periodically.

Use all available mediums to communicate: Disaster recovery team uses multiple mediums to deliver the changes so that information reaches to all the concerned individuals.

CONCLUSION

Business Continuity Planning (BCP) requires cross-functional team efforts. It is essential to communicate appropriately with all the stakeholders. The communication format should be simple and effective. If it is critical to have a BCP, it is even more important to keep it up to date and perform periodic dry runs and testing.

REFERENCES

1. Hiles A. The definitive handbook of business continuity management. John Wiley & Sons. 2010.
2. Merna T, Al-Thani FF. Corporate risk management. John Wiley & Sons. 2011.
3. Wilkinson JM, Estes D. New Madrid Seismic Zone:Catastrophic Planning Initiative. EIIP Virtual Forum. 2009.
4. Harrison C. Blog-The Effects of a Power Outage on a Business. 2008.
5. Arvig. Benefits and Bottom Lines on Backups. How to Choose a Data Recovery Solution. 2019.
6. Jablokow A. What is Virtual Infrastructure Management. 2018.
7. Avtech. How To Install Device ManageR. Knowledge Base.
8. Lynch W. The Natural Disaster Ripple Effect. 2018.
9. Gaddum R. Business Continuity and Disaster Recovery in the retails sector. International Journal of Retail & Distribution Management. 2002; 30(7).
10. Techrepublic. Disaster recovery and business continuity plan. 2020.
11. Bernstein C. Disaster Recovery Team. 2019.
12. Globalscape. Enterprise Data management. Retrieved from. 2018.
13. Acxiom. Customer data platforms. Data Management.
14. Juliana DG. Data Insider. 2021
15. Bloomberg. IT spending on rise at financial service firms, survey shows. 2007.
16. Thrivewpengine. Assured Disaster Time to Recovery. 2017.
17. Disastersafety. Preparing Your Business for a Severe Weather Emergency. 2020.
18. Gov au. Business Continuity Planning.
19. Jensenhughes. Business Continuity Planning During the Coronavirus. 2020.
20. Erin Sullivan. What is Business Continuity and why it is important. 2020.