Business Continuity Planning

TABLE OF CONTENTS

WHAT IS BUSINESS CONTINUITY PLANNING?

Business continuity planning is the process involved in creating a system of prevention and recovery from potential threats for a company or organization. A business continuity plan (BCP) is a set of plans in place that you can follow in order to keep particular business processes going in the event of a disruption. BCPs can and should be created for disruptions of all levels—from who is in charge when an executive goes on vacation to how to handle power outages to how to pivot in the midst of a global pandemic.

“It is crucial for the survival and growth of your business to get up and running as soon as possible.”

A disruption can be a huge crisis—such as a hurricane or Covid-19 or a cyber-attack—or something as simple as an employee vacation or a traffic accident making your place of business inaccessible. Regardless of the size of the disruptive event, it is important in these situations to have plans in place to empower your team and business to keep moving forward. It is crucial for the survival and growth of your business to get up and running as soon as possible. And this can only happen if all members in your team know their role and what to do in the midst of the disruption.

The act of putting together strategies to mitigate the risks from unexpected events is at the very heart of business continuity management. Business continuity helps preserve productivity and efficiency and peace of mind during emergencies. If you can enter the fray knowing that you have a plan in place, you will not be walking blindly.

Organizations that are not prepared to handle an array of disruptions (be they technological, manmade, or a weather phenomenon) can be left scrambling, risking employee health and client retention. Your plans should be personalized to meet the needs of your employees and the market you serve. They should be flexible as well..

“Your plans should be personalized to meet the needs of your employees and the market you serve.”

Developing a Business Continuity Plan:

In order to make sure your business continuity management takes a comprehensive approach; it should involve the following:

RISK ASSESMENT: This involves identifying potential threat to your business or processes. Your list may include anything from hacking to blizzards, sick employees to military conflict. If you identify a threat that could potentially impact your day-to-day operations, put it on the list.

BUSINESS IMPACT ANALYSIS (BIA): This should be a list of impacts to your business, such as loss of income, productivity or even your brand's reputation. You should create a BIA for each of your critical processes and systems.

DISASTER RECOVERY PLAN (DRP): Primarily a concern for IT, DRPs are put in place to recover your data, systems, applications. You can and should separate DRPs for each critical system and application.

BUSINESS CONTINUITY PLAN (BCP): These plans should be in place to ensure that a business process can continue, even if you don't have the people, workflows, or resources you would under normal circumstances.

CRISIS MANAGEMENT STRATEGY: This largely deals with the human side of the crisis. How do you ensure that your staff remains safe? Who talks to your vendors, customers, internal stakeholders and the media? What do they say?

BCPs are an important part of any business. Threats and disruptions mean a loss of revenue and higher costs, which leads to a drop in profitability. And businesses can't merely rely on insurance alone because it doesn't cover all the costs and the customers who move to the competition.

"Threats and disruptions mean a loss of revenue and higher costs, which leads to a drop in profitability."

Some additional steps that need to be taken in order to develop a business continuity plan include:

BUSINESS IMPACT ANALYSIS: This includes a business identifying functions and resources that are time-sensitive.

RECOVERY: In this portion of a BCP, the organization should identify and implement steps to recover critical business functions.

ORGANIZATION: A continuity team or continuity expert should be consulted. This person or team will devise a plan to manage the disruption.

TRAINING: The business continuity team must be trained, and the plan tested. Employees should also complete exercises that rehearse the plan and its strategies so that all stakeholders know what to do in a time of emergency. Amid a crisis is not the time to teach people how to react to said crisis. (For example, fire drills.)

It is useful to have the completed BCP also include a checklist that has key details such as emergency contact information, a list of resources that the continuity team may need, where backup data and other required information are housed, and other important personnel.

It is also important to test those responsible for implementing the BCP and ensuring that it can be applied to multiple risk scenarios. This will help identify any weaknesses in the plan which can then be identified and corrected. But remember, for any business continuity plan to be successful, all employees—even those who aren't on the continuity team—must be aware of the plan. Something as simple as having the foresight to print out the plan rather than it solely being digital is an example of something that could come up when testing the plan in the mock event of a power loss.

CHAPTER ONE: CONDUCTING A RISK ASSESSMENT

A risk assessment is about identifying all the possible threats to your business and its processes, from wherever they might originate. It is an important part of a thorough business continuity plan.

For example, if flooding from a hurricane wipes out a business's records and they don't have a backup site (or the backup is too close and is also flooded) the compliance issues from the destroyed records will linger for months and possibly even years afterward.

Whether the disaster is natural, like a hurricane or pandemic, or man-made, like a cyber-attack, it is important to identify and plan for situations where you may not have immediate access to the data, resources, staff, or even locations you are accustomed to during normal business operations. The goal of business continuity planning, after all, is to keep the business running no matter what happens. Therefore, it makes sense that we would take some time to address all the what-ifs and plan for those things.

"The goal of business continuity planning, after all, is to keep the business running no matter what happens."

The most common mistakes businesses make when it comes to business continuity planning and risk assessment include:

- Not accounting for loss of critical people.
- Not planning to accommodate the stress and trauma staff incur in a crisis.
- Not making the emergency plan easily accessible to staff at the office or working remotely or making plans that are too generic or are out of date.
- Failing to communicate plans and processes quickly and transparently and the resulting PR problems that can be related to recovery.
- No alternative emergency operation centers or recovery sites, or not having a plan for employees to work from home when a physical site isn't available.
- Believing that outside assistance and insurance will take care of everything.

During the risk assessment process, you must look within your organization to:

- Identify processes and situations that can cause harm, particularly harm to people.
- Determine how likely it is that each hazard will occur and how severe the consequences could be.
- Decide what steps the organization should take to prevent these hazards, control the risks, or mitigate bad possible outcomes.

The goal of a risk assessment plan will vary across industries, but overall, the goal is to help organizations prepare for and mitigate risk.

Other goals include:

- Providing an analysis of possible threats
- Preventing injuries or illnesses
- Meeting legal requirements
- Creating awareness about hazards and risks
- Creating an accurate inventory of available assets
- Justifying the cost of managing risks
- Determining the budget to remediate risks
- Understanding the return on investment

Before you begin the risk management process, you should determine the scope of the assessment, necessary resources, stakeholders involved, and the laws and regulations you will need to follow. Because the risk assessment process is so involved, it is most often best to consult with or hire a risk management specialist for this process.

“Because the risk assessment process is so involved, it is most often best to consult with or hire a risk management specialist for this process.”

5 STEPS IN THE RISK ASSESSMENT PROCESS

1. Identify the Hazards

Look around your workplace and see what processes or activities could potentially harm your organization. Include all aspects of work, including remote workers and non-routine activities such as repair and maintenance. You should also look at accident/incident reports to determine what hazards have impacted your company in the past.

These include but are not limited to natural disasters (i.e., hurricanes or fires), biological disasters (i.e., pandemics or foodborne illnesses), workplace accidents (i.e., slips, transportation accidents, or mechanical breakdowns), intentional acts (i.e., bomb threats, robbery or strikes), technological hazards (i.e., loss of internet connection or power and cyberattacks), chemical hazards (i.e., asbestos or cleaning fluid spills), mental hazards

(i.e., excess workload, sexual harassment, bullying), and interruptions in the supply chain.

2. Determine Who Might be Harmed and How

For every hazard that you identify in step one, think about who will be harmed should the hazard take place.

3. Evaluate the Risks and Take Precautions

Look at your list of potential risks and the effected people. How likely is it that the hazard will occur? How severe will the consequences be should the hazard occur? This evaluation will help you determine where you should reduce the level of risk and which risks should be deemed top priority.

4. Record Your Findings

If you have more than 5 employees in your workplace, you are required by law to write down your risk assessment process. Your plan should include the hazards you've found, the people they affect, and how you plan to mitigate all the risks. The record—or the risk assessment plan—should show that you:

- Conducted a proper check of your workplace
- Determined who would be affected
- Controlled and dealt with obvious hazards
- Initiated precautions to keep risks low
- Kept your staff involved in the process

This is a laborious process. We recommend using a specialized compliance specialist, like CentraVance Consulting, to help with this.

5. Review Assessment and Update if Necessary

Your workplace is always changing, so the risk to your business change as well. As new equipment, people, and processes are introduced, each brings the risk of a new hazard. Perhaps the new hazard is more widespread like the global pandemic Covid-19. To protect your business and its reputation, you must continually review and update your risk assessment process to stay on top of these new hazards.

By applying the risk assessment steps mentioned above and employing the help of a brand reputation specialist, you should be able to manage any potential risk to your business. Get prepared by completing a thorough risk assessment as a part of a larger business continuity plan. After all, luck favors the prepared!

“Luck favors the prepared!”

CHAPTER TWO: CONDUCTING A BUSINESS IMPACT ANALYSIS

It is 2020. Here is what we have learned: giant murder hornets are coming, we all love Hamilton, and if something can go wrong, it will. We have now come to expect the unexpected. And this is a great thing in terms of business continuity, especially when it comes to conducting a business impact analysis.

Business impact analysis (BIA) is a way to predict the consequences of disruptions to a business and its processes by collecting data which is then used to develop strategies for the business to recover in the case of emergency. All "what ifs" are explored, and possible threats and disruptions are identified. These can be as simple as delays in the supply chain and as complex as to what happens if there is a hurricane that knocks out your power in the middle of a pandemic and then the murder hornets invade. The list of possibilities is usually long (and may or may not always include the murder hornets), but it is key to explore all possible threats thoroughly in order to best assess risk. By identifying these possible threat scenarios, a business can then get to work addressing each one in order to either prevent them entirely or to come up with plans for recovery and mitigation strategies.

"Here is what we have learned: giant murder hornets are coming, we all love Hamilton, and if something can go wrong, it will."

The BIA should identify the operational and financial impacts resulting from disruptions to business functions and processes. It is also important to consider that these operational and financial impacts can vary based upon the timing of the disaster events. A disruption to your business just as things are ramping up for your "busy" season will obviously mean a greater financial loss than if the disaster occurs during a time of year where your business is more stagnant. A BIA will also help you identify which areas of your business must be prioritized in order to maintain business continuity.

"Identify which areas of your business must be prioritized in order to maintain business continuity."

A BIA should consider the impacts of the following based upon the identified risks:

- Loss of revenue
- Delayed sales or slower sales cycles
- Increased expenses
- Changes in regulations due to certain disasters and the costs associated with adhering to the new regulations
- Customer dissatisfaction
- Delay of new business plans or ventures

To conduct a BIA, use a simple questionnaire to survey stakeholders within the business. Survey those with inside knowledge of how the business works, its products, and services. They should identify what the potential impacts of disruptions of service would be and what is necessary to resume business function.

With the data gathered from the BIA questionnaire found at the end of this eBook, a report should then be written that documents the potential impacts resulting from business disruptions. Scenarios resulting in significant business interruption should then be assessed in terms of financial impact. These costs should then be compared with the costs for both risk prevention and possible recovery strategies. It should also prioritize the order of events for the restoration of day-to-day business operations. Business operations and processes with the greatest operational and financial impacts should be restored first.

“Business operations and processes with the greatest operational and financial impacts should be restored first.”

CHAPTER THREE: DISASTER RECOVERY PLANNING

Disaster Recovery Planning and developing a Disaster Recovery Plan (DRP) is a vital part of a Business Continuity Plan. A DRP ensures that all of your systems, data and personnel are protected. It makes sure your business continues to operate in the event of an emergency or disaster– be it hurricane, hacking, or the hindering high-jinks of 2020.

At this point in the business continuity planning process, you will have identified risks in a risk assessment. You will also have investigated who and how will be impacted in business impact analysis. Your DRP should include strategies to restore hardware, applications, and data in a timely fashion to meet the needs of your business continuity plan. A DRP seeks to aid an organization to resolve data loss and recover system functionality so that it can perform in the aftermath of an incident.

As cybercrime and security breaches become more complex and sophisticated, it is important for a business to define its data recovery and protection strategies. The ability to pivot quickly in the event of an emergency can reduce downtime and minimize damages to an organization's finances and reputation.

"A DRP ensures that all of your systems, data and personnel are protected."

Some types of disasters that a business should plan for could include:

- Application Failures
- Communication Failures
- Data Center Disasters
- Building Disasters
- Power Outages
- Ransomware Attacks
- Weather Emergencies
- National Disasters
- Active Shooters

DRP Considerations

A disaster recovery strategy should begin at the business level and determine which applications are most important to running the organization. The Recovery Time Objective (RTO) describes the target amount of time a business application can be down, and is typically measured in hours, minutes, or seconds. The recovery point objective (RPO) describes the age of files that must be recovered from backup storage for normal operations to resume.

Recovery strategies will define how an organization plans to respond to an incident, while disaster recovery plans will describe the how. A recovery plan flows from a recovery strategy.

When determining your organization's recovery strategy, the following should be considered:

- Budget
- Insurance
- Resources—people and physical facilities
- Technology
- Data
- Vendors and Suppliers
- Compliance requirements
- All strategies should align with the organization's overall mission and goals.

"Recovery strategies will define how an organization plans to respond to an incident."

Types of Disaster Recovery Plans

Disaster Recovery Plans can be specifically tailored for a given environment or business. Some specific examples for DRPs include:

- *Virtualized Disaster Recovery Plan:* Virtualization provides opportunities to implement disaster recovery in a more efficient and simpler way. Testing can also be easier to achieve, but the plan must include the ability to validate that applications can be run in disaster recovery mode and returned to normal operations within the RPO and RTO.
- *Network Disaster Recovery Plan:* Developing a plan for recovering a network gets more complicated as the complexity of the network increases. It is important to detail the step-by-step recovery procedure, test it properly and keep it updated. Data in this plan will be specific to the network, such as in its performance and networking staff.
- *Cloud Disaster Recovery Plan:* Cloud disaster recovery (cloud DR) can range from a file backup in the cloud to a complete replication. Cloud DR can save space, time, and money, but maintaining the disaster recovery plan requires proper IT management. The manager must know the location of physical and virtual servers. The plan must address security, which is a common issue in the cloud that can be alleviated through testing.
- *Data Center Disaster Recovery Plan:* This type of plan focuses exclusively on the data center facility and infrastructure. An operational risk assessment is a key element in data center DRPs. It analyzes key components such as building location, power systems and protection, security, and office space. The plan must address a broad range of possible scenarios.

Scope and Objectives of Disaster Recovery Planning

A DRP can range in scope from basic to comprehensive.

A DRP checklist includes identifying critical IT systems and networks, prioritizing the RTO, and outlining the steps needed to restart, reconfigure, and recover systems and networks. The plan should at least minimize any negative effect on business operations. All employees should know basic emergency steps in the event of an unforeseen incident.

How to Build your Disaster Recovery Plan

The DRP process involves more than simply writing the document. The DRP takes into account the previous steps in the business continuity planning process, such as the Risk Assessment (RA) and the Business Impact Analysis (BIA). The RA identifies threats and vulnerabilities that could disrupt systems of operations. The BIA identifies the impacts of disruptive events and is your starting point for identifying risk within the context of disaster recovery. It also generates the RTO and RPO.

“A good disaster plan is a constant evolution, a living document seeking the input and wisdom of all stakeholders.”

A DRP checklist should include:

- establishing the range or extent of necessary treatment and activity — the scope of recovery.
- gathering relevant network infrastructure documents.
- identifying the most serious threats and vulnerabilities, and the most critical assets.
- reviewing the history of unplanned incidents and outages, and how they were handled.
- identifying the current disaster recovery strategies.
- identifying the incident response team.
- having management review and approve the DRP.
- testing the plan.
- updating the plan.
- implementing a DRP audit.

A good disaster plan is a constant evolution, a living document seeking the input and wisdom of all stakeholders.

Another component of the DRP is a well thought out crisis communications plan. The crisis communications plan should detail how both internal and external crisis communication will be handled. Internal communication includes alerts that can be sent using email, overhead building paging systems, voice messages or text messages to mobile devices. Examples of internal communication include instructions to evacuate the building and meet at assembly points, updates on the progress of the situation and notices when it's safe to return to the building.

External communications are even more essential to the business's continuity plan and include instructions on how to notify family members in the case of injury or death; how to inform and update key clients and stakeholders on the status of the disaster; and how to discuss disasters with the media.

An effective disaster recovery plan defines the roles and responsibility of disaster recovery team members and outline the criteria requires to put the plan into action. The plan should then specify, in detail, the incident response and recovery activities.

Testing Your Disaster Recovery Plan

Testing your DRP identifies weaknesses and opportunities to fix problems before they occur. An easily recognizable example of this is a fire drill. Students know where to stand on the ball field because they have practiced it and stragglers can be identified and coached through the process. Testing can also offer proof that the DRP is effective and hits RPOs and RTOs. Because IT systems and technologies are constantly evolving, testing also helps make sure your DRP is up to date.

"Testing your DRP identifies opportunities to fix problems before they occur."

CHAPTER FOUR: A THOROUGH BUSINESS CONTINUITY PLAN

A business continuity plan (BCP) enables your organization to pivot smoothly in the midst of a crises—be it fire, hurricane, pandemic, or loss of power. Without a comprehensive business continuity plan in place, your business could lose profits, employees and/or clients could get hurt, your brand's reputation be damaged or even be forced to close. A thorough BCP helps to prevent the worst-case scenarios and keep the ball rolling.

Luckily, there are ample resources and service providers who can help you to create a BCP. As we have discussed, the first phase of business continuity planning includes a thorough risk assessment. Once a risk assessment has been conducted, you will be better able to list your organization's strategic objectives and then begin to make your plans. (Remember the ProActive Methodology? Strategy→ Plans→ People→ Process→ Tools & Technology? Yes, faithful reader. Our superpowers apply here too.) After your risk assessment, you will have conducted your business impact analysis (BIA). Your BIA basically takes all the "What if" scenarios from your risk assessment and defines how your business and its people and operations will be affected so that it can best prioritize its strengths and weaknesses and quantify just how big of a deal each of those risks are and to what areas.

"Yes, faithful reader. Our superpowers apply here too."

Your BIA will identify your core business operations and critical points for business continuity. This will help you make the most logical and realistic recovery plans while keeping in mind your risks. Your BIA will help you proactively identify potential problems that may arise. If any functions or departments have time-sensitive operations, monitor the tolerable downtime. Use a rating system for key business functions to help you understand where to allocate resources.

With all of this information in hand, now you can strategize. And then make plans. If X happens, we will do A, B, and C.

Your plans should be the most detailed portion of your Business Continuity Plan.

"Each department should have a detailed emergency response plan."

You will divide your strategies into three different categories: Prevention, Response, and Recovery.

Prevention Strategies:

What can you do to prevent threats? Your BIA will likely identify areas that need mitigation. This could include having back up power supplies, employees knowing who is next in line should an employee be out or making sure you have remote workstations ready should your employees need to telework.

Response Strategies:

Each department should have a detailed emergency response plan that includes exactly what each member of the team should do in the case of an emergency.

For example, if there is a fire, procedures and safety protocols are essential for recovery. How will each employee leave the building? Where will people gather? When, how, and who will alert the media, public or customers should also be

specified in your response strategies. This should also include a detailed disaster recovery plan to make sure all that your technology needs are covered and will probably require an IT strategy and management specialist.

It is important to remember to keep communications in mind. How you communicate what you do is key to maintaining your organization's integrity.

Recovery Strategies:

After the disaster has occurred, your organization's focus should be on recovery. This step of the business continuity plan outlines exactly what your recovery processes are and who is responsible for implementation.

Some resolutions and recovery steps will be instantaneous. Others may take days or weeks. For all of your recovery plans, make sure your stakeholders have clear-cut estimates on recovery plan activation.

Training and Testing:

Your BCP should include plans to train your team what to do in the event of an emergency. This could include basic training as well as individual trainings to specific threats, for example, training on what to do if an employee has been exposed to Covid-19 and other items pertaining to Covid-19. (This training is required for all businesses with over 5 employees in the Emergency Temporary Standard (ETS) in the Commonwealth of Virginia.)

As part of your BCP, you should also include tactical exercises designed to test procedures and protocols and to prepare employees. Examples of this include fire and active shooter drills.

Another element of this training should include developing a crisis communications plan and letting employees know who and who cannot speak for the company. It is best to instruct employees NOT to publish updates on Facebook, Twitter, or LinkedIn. Remember

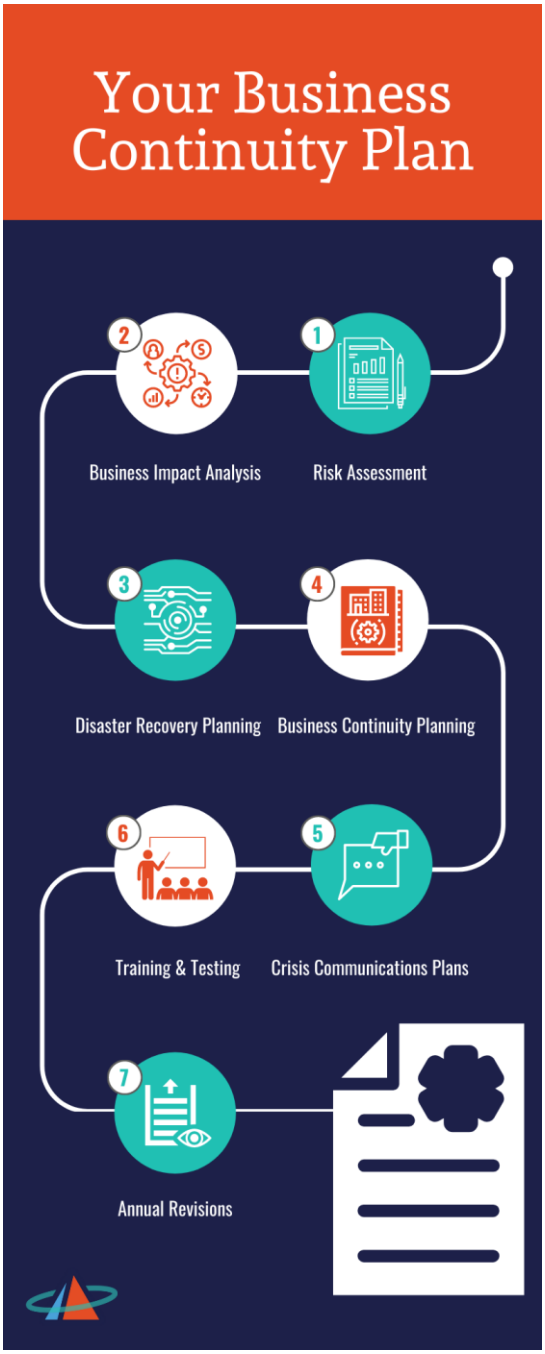
that your designated communications representative will be the one to speak for your company.

Your training exercises should have:

- Clear goals and objectives
- Easily understood descriptions of the emergency scenarios
- Instructions for all participants
- A post-exercise evaluation

Business continuity planning should evolve your organization and as new threats appear. You should conduct reviews of your BCP annually. These reviews and any updates made should be documented and your team should be made aware of them.

Having a concrete BCP in place is an essential security measure to protect your business, brand, and reputation. Having a dynamic plan in place can help build trust and confidence with employees and relevant stakeholders.



CHAPTER FIVE: CRISIS COMMS IN A BCP

Communicating amid a crisis that affects your business continuity is a delicate matter. They say it is not only what you say but how you say it that matters. The same idiom also holds true when it comes to communicating with your stakeholders in the event of a crisis. It not only matters what you do, but also how you communicate about what you are doing. Providing peace of mind in the midst of a crisis, making sure that others know there is a plan in place, and making sure that those in charge execute this plan is no small feat.

"It is not only what you say but how you say it that matters."

In order to address any threat to business continuity, your organization needs to make sure it has a crisis communications plan in place. Your business should speak with a unified voice and have a decided upon "front" person to whom the media or other stakeholders can address their questions. This person should be poised and may be your top public relations person or someone else within the C-Suite. From time to time, this person may also want to receive guidance or pass the baton to another subject matter expert, depending upon the context of a crisis. For example, if the crisis is security related, you may tap your Chief Security Officer to address the situation. With this in mind, it is important for all of your employees to know who these spokespeople are and for those spokespeople to have the tools at hand with which to create peace of mind in the middle of the crisis.

This is often best handled by having a boilerplate script and making sure that all involved have

immediate access to the appropriate communications channels.

As you prepare your business for this portion of its business continuity planning, it is necessary to consider the following questions:

Official Company Spokespeople:

- Who are the executives at the C-Suite level that are the subject matter experts in their fields?
- Who can make sure that all replies are in line with your company's goals, visions, and branding?
- Make sure that your employees know whom to contact in the event they are asked questions by clients and/or the outside media.

When planning for a crisis, it is vital to not only address who will speak on behalf of your organization to the outside world, but also to address internal communications.

Who will be in charge of making sure that employees know what is going on? This too should be a top down unified effort. Employees should be kept abreast of situations and it is critical that a plan is in place to disseminate accurate information in a timely manner. For example, in the event of a natural disaster like a hurricane, the head of PR may alert the media as to whatever closings or outages your company is facing, whereas the head of HR makes sure that employees are aware of those same outages and whatever policies need to be followed. Make sure that this person is also aware of the appropriate means of communications with employees—perhaps it is Microsoft Teams, Slack, Email or Text messaging. This person needs quick access to the employee directory.

"Who will be in charge of making sure that employees know what is going on?"

Channels of Communication:

Your first task should be to alert your clients that you are aware of the crisis and that you are in the process of handling it. You have a business continuity plan in place—have no fear! Do not wait until you have all the answers to communicate with your clients. You can buy yourself time to figure out all the answers through a thorough investigation by letting stakeholders know that you are addressing the crisis. By being transparent, you will build trust. Don't forget to update other company forms of communications such as your website and outgoing voicemails, if appropriate.

If you have a social media manager, your head spokesperson should work with her to craft contextually appropriate messages for all your organization's social media platforms. Remember, the audience for each channel is different, so while the tone of each message should be different, the voice should be cohesive.

Script:

Make sure that your company's mission and vision is ever before you as you craft your message when responding to client and media inquiries during a time of crisis, including tone and language. It may be helpful to also have boilerplate messages crafted for more predictable crises such as natural disasters or a disgruntled customer.

By using crisis communications best practices, you should be able to pivot confidently in the event of a crisis and implement your business continuity plan effectively. Remember, above all else, your communication should be honest, human, and timely.

"You have a business continuity plan—have no fear!"

CHAPTER SIX: BCP IN THE TIME OF COVID-19

On July 15, 2020, Virginia became the first state in the nation to implement an emergency temporary standard (ETS) to address the COVID-19 pandemic. The ETS covers *every employer* in the Commonwealth and includes *mandatory* requirements for all employers (with additional requirements for workplaces with certain exposure risk levels), training and leave requirements, and an anti-discrimination provision.

The ETS took effect the week of July 27,2020. Once in effect, employers have 30 days to comply with the training requirements on the ETS and 60 days to comply with the training requirements on the employer's infectious disease preparedness and response plan.

The ETS requires each employer to assess the "exposure risk level" of disease-related hazards present for job tasks undertaken by employees at each place of employment. The exposure risk levels articulated in the ETS are "very high," "high," "medium," and "lower." The ETS defines factors that employers should consider when assessing their exposure risk levels but also defines these risk levels.

The ETS indicates that, to the extent an employer "actually complies with requirements contained in CDC publications, whether mandatory or non-mandatory to mitigate SARS-CoV-2 virus and COVID-19 disease related hazards or job tasks addressed by this [ETS], the employer's actions shall be considered in compliance with this [ETS]." The ETS does not, however, identify what constitutes a "CDC publication" nor does it explain how the state will decide whether an employer is complying with any such CDC publications. The ETS says that compliance with the CDC mandatory and

non-mandatory guidelines *does not indicate compliance with ETS* but will be a factor of consideration in any enforcement action. Organizations must have documented plans and policies to demonstrate compliance. No one takes your word for it.

“Organizations must have documented plans and policies to demonstrate compliance. No one takes your word for it.”

Despite the exposure risk levels that a workplace falls under, the ETS contains certain mandatory requirements for all employers in Virginia. These include:

- Conducting an exposure assessment of all workplaces & classifying each job task according to the exposure hazards.
- Informing employees of the methods of contracting COVID-19 and encouraging employees to self-monitor for signs and symptoms.
- Developing and implementing policies & procedures for employees to report when they're experiencing symptoms consistent with COVID-19.
- Prohibiting employees or other persons known or suspected to be infected with the virus from reporting to or remaining at the work site until cleared to return to work.
- To the extent feasible & permitted by law, ensuring that sick leave policies are flexible & consistent with public health guidance & that employees are aware of these policies.
- Discussing with subcontractors & companies providing contract or temporary employees about the importance of employees staying home if they are suspected or known to have COVID-19.
- To the extent permitted by law, establishing a system to receive notice of any positive SARS-CoV-2 tests by employees, subcontractors, contract employees, & temporary employees who were present at the place of employment within the 14 days preceding the positive test and provide certain notifications to their own employees, the employees of others, the building/facility owner, the Virginia Department of Health, and the Virginia Department of Labor & Industry, depending on specific circumstances articulated in the ETS.

The ETS contains mandatory requirements for all employers in Virginia (continued):

- Ensuring employees have access to their own virus & disease-related exposure & medical records.
- Developing and implementing policies & procedures for employees to return to work.
- Ensuring employees observe physical distancing on the job & during paid breaks.
- Closing or controlling access to common areas.
- Ensuring compliance with respiratory protection when multiple employees are occupying a vehicle for work purposes.
- Ensuring compliance with respiratory protection when the nature of an employee's work or work area does not allow physical distancing.
- Complying with specific sanitation & disinfection requirements articulated in the ETS.

The ETS also requires additional engineering and administrative controls to be implemented depending on the job task or hazard's exposure risk level.

As for training requirements, Virginia employers *must train their employees on the ETS* and may also be required to develop and implement a written Plan with very specific issues to be addressed in such Plan and to train their employees on this Plan as well.

Finally, the ETS contains an anti-discrimination provision that prohibits employers from discharging or discriminating against employees exercising their rights under the ETS, voluntarily wearing their own personal protective equipment, and raising a "reasonable concern about infection control related to COVID-19."

CentraVance Consulting has created a COVID-19 Coverage service for you, so you can comply with the new ETS and protect your brand and reputation. The COVID-19 Coverage package includes:

- Training on Infection Control, Pandemics, and Responses
- Policy that is specific to your practice and your needs
- Identification of risk levels
- Identification of control measures
- Emergency Procedures
- Infectious disease exposure and return to work protocol
- Posters and forms

CentraVance

Business Impact Analysis Worksheet

Department/ Function/ Process _____

Operational & Financial Impacts

Timing/Duration	Operation Impacts	Financial Impact

Timing: Identify Point in time when interruption would have greatest impact (e.g., season, end of month, quarter)
Duration: Identify the duration of the interruption or point in time when the operational and/or financial impact(s) will occur.
Operational Impacts: Loss of revenue, Delayed sales or slower sales cycles, Increased expenses, Changes in regulations due to certain disasters and the costs associated with adhering to the new regulations, Customer dissatisfaction, Delay of new business plans or ventures
Financial Impacts: Quantify operational impacts in financial terms.

CRISIS COMMUNICATIONS TEMPLATE

Crisis Communications Plan Template

Official Company Spokespeople:
List Name, Phone, and Email contact information

Head of PR: _____
Legal: _____
IT: _____
HR: _____
Logistics: _____
Security: _____
Internal Communications: _____

Channels of Communication:
These channels should have contextual messaging but be unified in their message

- ❑ **Email/Phone/Text Clients**
- ❑ **Website Update**
- ❑ **Update Outgoing Voice Mail**
- ❑ **FB:**
- ❑ **Twitter:**
- ❑ **LinkedIn:**
- ❑ **Instagram:**
- ❑ **TikTok:**
- ❑ **Pinterest:**
- ❑ **CBS:**
- ❑ **NBC:**
- ❑ **ABC:**
- ❑ **Local Newspaper:**
- ❑ **Other:**

Script:
(DO NOT SAY "NO COMMENT"!)

"We are aware there *may* be a problem and we are investigating the situation with the appropriate parties. We intend on making more details available within the next 24 hours."

But remember: if you are not the appointed spokesperson for the company and have not been asked to speak on behalf of the company, you are not to do so.