




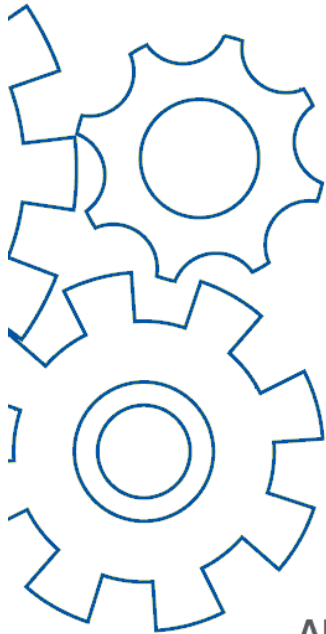
NATIONAL ASSOCIATION OF
Community Health Centers®



**BUSINESS CONTINUITY
PLANNING
INTERACTIVE LEARNING
MODULE ONE**

INTRODUCTION TO BUSINESS CONTINUITY PLANNING

AUGUST 2022



ABOUT THESE INTERACTIVE LEARNING MODULES

- These learning modules are the result of collaboration between the National Association of Community Health Centers (NACHC), Connecting Consulting Services, and Primary Care Development Corporation (PCDC), and Inspired Solutions Enterprises, Inc.
- They are intended to provide community health centers and primary care associations with self-guided learning tools to create and/or improve their business continuity plans and programs.
- For assistance, questions or more information on this and other business continuity and emergency preparedness tools and resources, please contact NACHC at trainings@nachc.org or 301-347-0400.

This publication is supported by the Centers for Disease Control and Prevention of the U.S. Department of Health and Human Services (HHS) as part of a financial assistance award totaling \$2,000,000, with 100 percent funded by CDC/HHS. The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement, by CDC/HHS, or the U.S. Government

BUSINESS CONTINUITY PLANNING

INTERACTIVE LEARNING MODULE 1

INTRODUCTION TO BUSINESS CONTINUITY PLANNING

Overview

Business continuity planning (BC planning) is the process of defining systems for mitigation and recovery to deal with potential threats to an organization. The Business Continuity Plan (BCP) is a framework for the continuity of pre-identified essential business functions and identified associated dependencies, recovery times and impact scores as well as to define cross-departmental components that support an organization as they begin the process of disaster recovery. A fully executed BCP will address the necessary elements health centers need to maintain their essential business functions following a disaster.

After a disaster, according to the Federal Emergency Response Administration (FEMA), of businesses without a BCP, 43% close and never reopen, 51% close within 2 years and 75% of fail within 3 years following the disaster.¹ Business Continuity Plans are intended to prepare and provide guidance to the health center during a disaster to continue providing patient care, minimizing negative financial impact and maintain operations. Comprehensive BCPs also address Disaster Recovery Planning which is focused on returning the health center to normal operations as quickly as possible following a disaster.

This course will review the rationale, scope, and components, and the recommendations and resources that are required to support the efficient development of a comprehensive BCP. This learning experience is made up of three modules:

MODULE 1: INTRODUCTION TO BUSINESS CONTINUITY PLANNING (1.5 HRS)

MODULE 2: CREATING A BUSINESS CONTINUITY PLAN (2 HRS)

MODULE 3: ENSURING A HUMAN RESOURCE STRATEGY (1 HR)

Together, these three modules provide guidance and resources for facilitating the development of a comprehensive health center BCP. Module 1 offers a comprehensive introduction that all members of the health center leadership team and board would find useful. Modules 2 and 3 provide more specific guidance for the BC planning leader and team.

Course Learning Objectives

Upon completion of these modules, learners will be able to:

1. Discuss the definition and rationale for BCPs
2. Describe the components of a comprehensive BCP
3. Draft a comprehensive BCP

Note:

1. FEMA Business Continuity Planning Suite. Business Continuity Training Part 2: Why is Business Continuity Planning Important? <https://www.youtube.com/watch?v=PDW4luQneeQ>

DISCLAIMER: Resources originating from organizations other than NACHC are being provided as a convenience and for informational purposes only; they do not constitute an endorsement or an approval by NACHC of any of the products, services or opinions of the corporation or organization or individual.

MODULE 1: INTRODUCTION TO BUSINESS CONTINUITY PLANNING

Overview of Module 1

Module 1 introduces a framework for the development of a BCP for health centers. BCPs are intended to prepare and provide guidance to the health center during a disaster to continue providing patient care, minimize negative fiscal impact and maintain operations.

Recommended Audience

Health center leaders, participating members of the board of directors, staff assigned to developing the business continuity planning process

Module Objectives

Upon completion of Module 1, learners will be able to:

1. Define and provide a rationale for business continuity planning
2. Describe the major components and considerations of business continuity planning, including regulatory requirements, and staff and board roles
3. Highlight staff, tools, resources, and board support required

Module 1 Chapters

- | | |
|--|--|
| 1. Introduction | 10. Cybersecurity Risks |
| 2. Business Continuity Planning Is... | 11. Making the Business Case for Business Continuity Planning |
| 3. Relevant Regulations | 12. Frequently Asked Questions |
| 4. Disaster Classifications | 13. Knowledge Check |
| 5. Characteristics of Business Continuity Plans | 14. Preparation for Module 2: Creating a Business Continuity Plan |
| 6. Business Continuity Plan Components | |
| 7. Business Continuity Planning Strategies | |
| 8. Business Continuity Planning Team | |
| 9. Board of Director Roles in Business Continuity Planning | Appendix A: Glossary of Business Continuity Planning Terms
Appendix B: Business Continuity Planning Resources Toolbox |

Structure of the Chapters

Following an introduction, the major content is organized by chapter titles in the left column. Additional learning and integration activities related to the chapter are located in the right column under "Go Deeper." The number and type of activities accessed by the learner in the Go Deeper column will depend on the learner's goals and prior knowledge. Completing the Listen, Discussion, and Activity(ies) in the Go Deeper column will result in the completion of module objectives.

CHAPTER (MAIN CONTENT)	GO DEEPER (LEARN MORE, DO THE WORK)
------------------------	-------------------------------------

Module 1 Time Commitment: 1.5 Hour Minimum

The actual amount time required to complete this self-paced, self-directed learning experience is variable depending upon many factors, such as learning goals, prior knowledge, how many of the Go Deeper activities and resources are utilized, and the degree to which the activities are completed as a team. Expect this module to require a minimum of 1.5 hour to review the main content areas and embedded audio/video files and complete the Knowledge Check.

"If you fail to plan, you are planning to fail."

Benjamin Franklin



This video, produced by FEMA as part of its Business Continuity Planning Suite is a humorous, but serious look at the purpose and value of Business Continuity Planning. View the full video on YouTube: Ready.gov - Business Continuity Training Introduction (3:30 min) https://www.youtube.com/watch?v=R1oIQ4Y_EHY&list=PL720Kw_Oojly2uSz0VTHM-Whk-Su8Ucy&index=1

CHAPTER 2 | BUSINESS CONTINUITY PLANNING IS...

GO DEEPER

• What is Business Continuity Planning? Why is it Important?

Business continuity (BC) planning is a process that outlines the potential impacts of an unplanned disruption in operations and identifies the steps organizations will take to prepare for, respond to, recover from, and mitigate potential impacts *in advance of the emergency situation/disaster*. Business continuity plans (BCPs) are more than a “nice to have,” they are essential to the operations planning of the health center.

Although there is some overlap, the BCP and Emergency Response plans are different. When responding to a disaster these plans will be activated simultaneously as they work together to address a disaster. Emergency response plans focus on the safety and protection of life, assets, and the environment. On the other hand, business continuity focuses on continuing the operations of the health center until it can return to normal.

Before, during and following a disaster, BCPs allows organizations to:

- Maintain or restart business operations efficiently
- Build patient confidence in the health center’s ability to continue to meet their health needs
- Build staff confidence in the health center’s ability to continue to operate efficiently and be prepared to meet their needs as employees
- Protect their supply chains
- Mitigate financial risk
- Mitigate cybersecurity risk

BCPs are realistic, dynamic, responsive to change and maintain relevancy for current times. They are not intended to be an exhaustive “how to” manual, but rather to act as a realistic guide for good decision making, preparation for disasters, and to direct the actions of staff in the immediate aftermath of a disaster.

While it is nearly impossible to predict with a high degree of certainty what type of disasters may strike, their timing, severity, impact, and duration; BC planning will help your health center be as prepared as possible with the resources and procedures for successfully recovery.



Business continuity planning helps ensure business resiliency in the face of disaster.



LISTEN

[What is the difference between an Emergency Response Plan and a Business Continuity Plan?](#) (2 min). Amanda Cooper, MPH, Planning Specialist, Connect Consulting Services



VIEW

[Business Continuity Planning Suite. Business Continuity Training Part 2: Why is Business Continuity Planning Important?](#) (5 min) FEMA.

Business Continuity Institute Webinar Series Session 1: Introduction to Business Continuity Planning. NACHC, 2021.

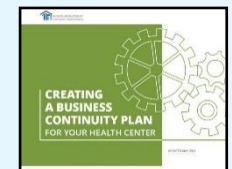
[Webinar](#) (60 min)
[PowerPoint Slides](#)







READ/REFERENCE

[Creating a Business Continuity Plan for Your Health Center.](#) NACHC. May 2021 (PDF).

- Business Continuity Plan vs. Emergency Operations Plan, Appendix M, p. 38



[Healthcare Business Continuity Management and Disaster Recovery— No Longer an Afterthought in Today’s World.](#) Association of Healthcare Internal Auditors (AHIA) and Crowe. (PDF)

CHAPTER 3 RELEVANT REGULATIONS	GO DEEPER	
<ul style="list-style-type: none"> <p>FQHC CMS Emergency Preparedness Final Rule § 491.12 “The Rural Health Clinic/Federally Qualified Health Center (RHC/FQHC) must comply with all applicable Federal, State, and local emergency preparedness requirements. The RHC/FQHC must establish and maintain an emergency preparedness program that meets the requirements of this section.”</p> <ul style="list-style-type: none"> ○ FQHCs must develop and maintain an emergency plan that includes continuity of operations, including delegations of authority and succession plans ○ Continuity of operations planning generally considers elements such as: essential personnel, essential functions, critical resources, vital records and IT data protection, alternate facility identification and location, and financial resources ○ Facilities are encouraged to refer to and utilize resources from various agencies such as FEMA and Assistant Secretary for Preparedness and Response (ASPR) when developing strategies for ensuring continuity of operations ○ Well-written, comprehensive BCPs may fulfill this requirement <p>Other Related CMS Requirements</p> <ul style="list-style-type: none"> ○ § 482.15 (a) 1 ○ § 482.15 (a) 2 ○ § 482.15 (a) 3 ○ § 482.15 (a) 4 ○ § 422.504(o) ○ § 423.505(p) ○ § 422.100 <p>The Joint Commission “Hospitals should identify potential hazards, threats, and adverse events and assess their impact on the care, treatment, and services provided for their patients. This assessment is known as a Hazard Vulnerability Analysis (HVA) and is designed to assist hospitals in gaining a realistic understanding of their vulnerabilities in order to help them mitigate and respond to emergencies and their subsequent impact.”</p> <p> FQHCs are required by law to develop and maintain a plan for continuity of operations during emergencies/disasters.</p>	 <p style="text-align: center;">Read</p>	<p>READ/REFERENCE Rural Health Clinic / Federally Qualified Health Center Requirements CMS Emergency Preparedness Final Rule Updates Effective March 26, 2021 (PDF)</p> <p>The Joint Commission Emergency Management Requirements (PDF)</p>
	 <p style="text-align: center;">Listen</p>	<p>LISTEN The CMS Emergency Preparedness Final Rule (2 min). Nora O’Brien, MPA, CEM, Founder and CEO Connect Consulting Services</p>
	 <p style="text-align: center;">Activity</p>	<p>ACTIVITY Find out if your health center is currently in compliance with FQHC CMS Emergency Preparedness Final Rule § 491.12.</p>

CHAPTER 4 | DISASTER CLASSIFICATIONS

GO DEEPER

- **What are the Classifications of Disasters?**

Health centers may be subject to a variety of disaster types. Preparation, response, recovery and mitigation may vary based on the type of disaster and chances that it may impact the health center. Assessment of risk for types of disasters occurs during the Hazard Vulnerability Assessment of the planning phase. There are several different ways to classify disasters, however, the following two categories cover the fundamental types:

- *Natural Disasters* are major adverse events that are caused by large-scale biological, geological, or meteorological changes in the earth, such as tornadoes, severe storms, earthquakes, droughts, floods, hurricanes, tropical storms and pandemics
- *Human or Human-caused Disasters* are directly or indirectly caused by people, and include events such as mass shootings, acts of terrorism, cyber-attacks, biological weapons, chemical spills, drought due to over-consumption, landslides due to extensive deforestation, etc.

- **In What Ways Might Disasters Impact Health Center Operations?**

Common scenarios resulting from disasters that can cause a health center to be inoperable include:

- Critical staff and/or vendors are unavailable or cannot be contacted
- Facility or the local community area is not accessible
- Equipment is not working at the health center
- Software is ruined or not working due to hardware issues or a cyber security attack
- Critical data and records are unavailable or destroyed
- Utilities are down



Disasters take many forms, including those that are considered “natural” and human caused. Hybrid disasters are sometimes recognized to be a combination of both human-caused and natural disasters. Health center operations can be severely impacted in different ways by any number of disasters.



READ/REFERENCE

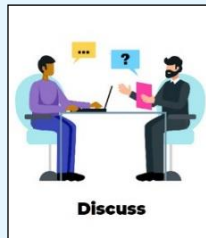
[Types of Disasters](#), SAMHSA.



ACTIVITY

Use the following resources to identify the most likely disasters in your local area:

- [Common Disasters Across the U.S.](#) American Red Cross. Learn what disasters are most common in your region.
- [Interactive Disaster Map.](#) The Ready Store. Learn the likelihood of specific natural disasters affecting your state.
- [Disaster Declarations for States and Counties.](#) FEMA. Explore historic federal disaster declarations by state, county, hazard, and year.



DISCUSS & DO

Discuss the following questions with your peers and document the responses:

1. *What disasters have already occurred or are likely to occur that may impact my health center? Note, if your health center has not experienced a disaster in recent years, consider using one or more of the following scenarios:*
 - a. *Power grid failure lasting more than 5 days*
 - b. *Tornado destruction of part of the health center and community*
 - c. *Ransome Ware attack on patient information systems*
 - d. *Ebola Virus Disease outbreak*
2. *What was the impact of the disaster on Patient care? Staffing? Data security? Supplies? Financial impacts? Others?*
3. *Was my facility prepared? How long did it take to recover?*
4. *What did we learn?*

CHAPTER 5 | CHARACTERISTICS OF BUSINESS CONTINUITY PLANS

• **Effective Business Continuity Plan Characteristics**

- Ensure health centers can restore operations quickly following a disaster
- Are comprehensive, realistic, efficient, and adaptable and realistic
- Address all of the disasters identified that may disrupt operations
- Are developed and ready to implement *before* disaster strikes, during "Sunny Skies"

"The time to repair the roof is when the sun is shining."

— John F. Kennedy —

• **Why Plan During Sunny Skies?**

- Allows adequate time to plan
- Provides opportunities to test and update plans
- Allows time to train staff and prepare the health center for potential disasters



BCPs are like insurance policies for disaster – it's better to have it in advance of a disaster than to have to develop it in the midst of one!

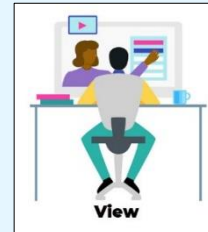
GO DEEPER



LISTEN

[How the Utah Navajo Health Systems Adapted to the Demand for COVID-19 Testing and Triage](#) (2 min). Amanda Cooper, MPH, Planning Specialist, Connect Consulting Services.

[Advance Planning During "Sunny Skies"](#) (3 min). Nora O'Brien, MPA, CEM, Founder and CEO Connect Consulting



VIEW

[PrepTalks: Human Biases: Why People Underprepare for Disasters](#) (22 min). FEMA.

Dr. Howard Kunreuther, Co-Director of the Wharton Risk Management and Decision Processes Center presents information on why humans don't prepare for low probability, high impact events. In his PrepTalk, he discusses human biases in decision-making under uncertainty including myopia, amnesia, optimism, inertia, simplification, and herding. He also proposes a behavioral risk audit that joins protective decision-making with economic incentives, enabling individual and collective actions to achieve greater resilience.



DISCUSS & DO

Discuss the following questions with your peers and document the responses:

1. *What are the likely barriers the BCP planning team will encounter while developing your health center's comprehensive BCP?*
2. *How will you manage these barriers?*

CHAPTER 6 | BUSINESS CONTINUITY PLAN COMPONENTS

- **What are the Components of a Comprehensive BCP?**

Comprehensive BCPs are individualized for each health center, including the content areas and format. *Generally*, BCPs will include the following components:

- Executive Summary
- Acknowledge Multidisciplinary Team Members/Contributors
- Hazard Vulnerability Analysis Summary
- Cybersecurity Impact Analysis Summary
- Human Resources Impact Analysis Summary
- Business Impact Analysis Summary
- Leadership Orders of Succession/Delegation of Authority
- Mitigation plan/strategy for all identified risks
- Recovery Strategies
- BCP Sustainability Strategies
- Implementation Timeline



There are many components to the BCP. Each health center will identify the components necessary to develop their individualized comprehensive plan. No two BCPs are the same.



GO DEEPER

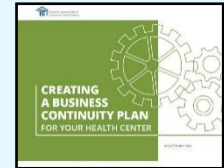
READ/REFERENCE

Sample Health Care Business Continuity Plans:

- [Business Continuity Plan Example A](#) (DOCX)
- [Business Continuity Plan Example B](#) (DOCX)
- [Good Samaritan Hospital: Business Continuity Guide for Critical Business Areas](#) (PDF - Sample/Template).

Business Continuity Planning Toolkits/Templates

- [Creating a Business Continuity Plan for Your Health Center](#). NACHC. May 2021 (PDF)
- [Continuity Plan Template and Instructions for Non-Federal Entities and Community Based Organizations](#). FEMA, August 2018.
- [Business Continuity Planning Suite](#). FEMA.
- [Hospital Continuity Planning Toolkit](#). California Hospital Association Hospital Preparedness Program Hospital Continuity Planning Workgroup. 2012. (PDF)



CHAPTER 7 | BUSINESS CONTINUITY PLANNING STRATEGIES

GO DEEPER

- **What are the General Strategies or Processes Used to Create a BCP?**

The strategy and process each health center uses to develop their BCP will be individualized based on resources available and level of urgency/importance for creating the plan. The general strategy typically incorporates the following activities:

- Secure senior leaders and Board of Directors' support for the staff involved in developing the plan and funding for needed resources
- Designate a BC planning leader, multidisciplinary BCP team, and acknowledge time commitments (e.g., regular schedule of meetings and time to work on the plan)
- Identify types of disasters to be considered in the plan
- Conduct vulnerability and impact analyses
 - Hazard Vulnerability Analysis (HVA)
 - Cybersecurity Impact Analysis (CIA)
 - Business Impact Analysis (BIA) – including both critical and non-critical processes and how limits of time and data may impact them
 - Establish a Recovery Point Objective for data
- Identify preparation, mitigation, and recovery strategies
- Delineate sustainability procedures, including policies and ongoing roles and responsibilities
- Develop implementation procedures and schedule
- Establish schedule for training, drills, routine review and procedures for debriefing after a disaster or drill
- Document the plan
- Educate the organization and community



There are many detailed planning and documentation activities needed to complete the BCP. Consistency in allocation of time and attention to the development of the plan are critical elements needed for successful completion of the BCP.

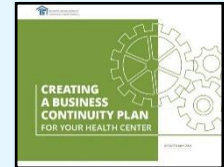


READ/REFERENCE

[Creating a Business Continuity Plan for Your Health Center](#). NACHC. May 2021 (PDF)

[Guide to Developing an Effective Business Continuity Plan](#). Noggin, 2020 (PDF)

[Healthcare Business Continuity Management and Disaster Recovery— No Longer an Afterthought in Today's World](#). Association of Healthcare Internal Auditors (AHIA) and Crowe (PDF)



CHAPTER 8 | BUSINESS CONTINUITY PLANNING TEAM

• BC planning Team Members - Who Should Be Involved?

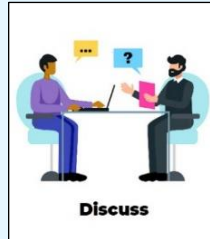
The core team should include a **designated, internal business continuity planning leader** and key leaders from across the health center, such as:

- C-Suite/Executive Offices
- Patient Care
- Operations
- Risk Management
- Information Technology
- Safety
- Human Resources
- Public Information
- Finance
- Legal
- Facilities
- Selected Critical Service Lines/Ancillary Departments
- Other functions as deemed necessary



The composition of the multidisciplinary team will be dependent upon available resources and strategies the health center adopts to create the plan. Critical to the team is an assigned BC planning leader.

GO DEEPER



DISCUSS & DO

Who are the potential leaders and members of your Business Continuity Planning Team? Consider:

1. *Who is in the best position to lead the BC planning Team? Think about scope of responsibilities/influence of their current job, length of tenure, familiarity with BCPs, availability and desire to lead the planning process.*
2. *What resources/allowances will the BCP team leader need to be effective?*
3. *Which key health center leaders/departments/functions are central to the development of the comprehensive BCP?*
4. *Which health center leaders/staff may be called upon for contributions to specific components of the plan?*

CHAPTER 9 | BOARD OF DIRECTOR ROLES

GO DEEPER

• Board of Directors Roles and Responsibilities

The essential roles of the Board of Directors are to ensure that the health center is prepared to handle any disruption and remain prepared to act in the event of a disaster.

- While the Board is involved more heavily during the initiation and development of the BCP, their ongoing roles and responsibilities for BC planning include:
 - Review, approve and support budgets for development and maintenance
 - Maintain oversight of the planning process, participate in the vulnerability and impact analyses workgroups
 - Connect the health center to community resources and other funding sources
 - Provide consistent support for training, assessment, and monitoring, and maintenance of emergency preparedness and BCPs
 - Review and acknowledge routine and emergency revisions to the plan



DISCUSS & DO

As you think about how you will engage the Board in the BC planning process, consider these questions:

1. *What issues do you expect the Board to raise concerning the development of the BCP? What are the key arguments for convincing the Board that a BCP is needed?*
2. *What information/resources can specific board members provide to support the development and sustainability of the BCP?*






ACTIVITY

Make a list of your concerns, questions, and requests for your Board. Identify strategies for engaging them in the process and supporting the development and implementation of the BCP.



The Board of Directors largely plays an oversight, guidance, resource identification/recommendation and allocation role in the development of the BCP.

CHAPTER 10 CYBERSECURITY RISKS	GO DEEPER	
<ul style="list-style-type: none"> Understanding Cybersecurity Risks Organizations of all sizes face many types of cybersecurity threats, and each type of threat must be approached using different tools. Health care organizations are “high value” targets for hackers due to the large amount of personal and financial information housed in the IT systems. 		<p>LISTEN Understanding Cybersecurity Risks (3 min). Nora O’Brien, MPA, CEM, Founder and CEO Connect Consulting Services</p>
<ul style="list-style-type: none"> Examples of Cybersecurity Vulnerabilities <ul style="list-style-type: none"> Employee / End User Errors: these errors are the top cause of the introduction of malware into the IT system and subsequent data breaches or disruption of service Point of Sale (POS) Intrusions: data mining from point-of-sale terminals Insider Threat: employees who have the intent to steal or corrupt data Web Application Attacks: include malware, phishing, and stolen access credentials that allow hackers to access business assets External Devices: create opportunities for data breaches when connected to the health center IT system Health Center Device Loss and Theft: includes items such as smartphones, tablets, and laptops Distributed Denial of Service (DDoS) Attacks: uses a network of computers to overload the health center’s website or software Strategies to Decrease Cybersecurity Risk Include: <ul style="list-style-type: none"> Utilize antivirus/malware detection products on <i>all</i> company and user-owned devices Utilize full encryption on all data Train everyone: utilize cybersecurity checklists, a cybersecurity action plan, and regular training for all staff on what to do and what not to do Verify compliance through routine security checks <p> Health center data is critical for operations and is a desired target for cyber criminals. Protection and recovery of data in the event of a disaster must be a top priority for the safety and security of all concerned.</p>		<p>READ/REFERENCE Cybersecurity in Healthcare The Healthcare Information and Management Systems Society (HIMSS). Cybersecurity in healthcare involves the protecting of electronic information and assets from unauthorized access, use and disclosure. The Healthcare Information and Management Systems Society (HIMSS) discusses the three goals of cybersecurity: protecting the confidentiality, integrity and availability of information, also known as the “CIA triad.”</p>

CHAPTER 11 | MAKING THE BUSINESS CASE FOR BC PLANNING

GO DEEPER

Justifying the Cost of BCP

BC planning requires a significant investment in both time and money on the part of the health center. By far, the greatest cost is of staff involved in the planning process. Additional costs should be factored in if health center decides to seek external consulting support. Advanced planning and strategic engagement of staff members in the planning process will help mitigate the expenses.

FQHCs are required by law to develop and maintain an emergency plan that includes **continuity of operations**. A well-developed BCP meets this requirement.

BC planning is ultimately justified by the positive impact it has on maintaining/resuming normal operations during a disaster.

- o The act of planning enables the health center to be better able to respond to a disruption, even if the type of disruption is not specifically stated in the plan.
- o The act of BC planning requires a good understanding of existing operations. Oftentimes, the process of BC planning helps to uncover and address operational gaps, poor practices, and wasted resources.

Consider Developing a Business Case for BC planning, if Needed

The Business Case answers the question: "What will happen if we approve or decline this investment decision?" It identifies the benefits and risks involved, recommendations and alternatives; and the risks of not proceeding. A strong business case will make a compelling recommendation for approval and implementation.



The cost of developing and maintaining a BCP is justified in the operational efficiencies gained during both disasters and normal operations.



LISTEN

[Unexpected benefits of BC planning](#) (3 min). Nora O'Brien, MPA, CEM, Founder and CEO Connect Consulting Services.



READ/REFERENCE

[How to Make a Business Case \(Workfront.com\)](#). Template for making a business case.



ACTIVITY

Familiarize yourself with the components and processes associated with the development of a business case in [How to Make a Business Case \(Workfront.com\)](#). Determine if a business case or components of a business case are needed to justify the resources and time required to create a BCP, and list the components you will include in the BCP. Be prepared to write the business case, if necessary.

CHAPTER 12 | FREQUENTLY ASKED QUESTIONS

QUESTIONS	ANSWERS
1. <i>How often should BCPs be reviewed?</i>	In most cases, you should conduct an annual review and update in addition to reviewing and updating the plan after each disaster or drill. Debrief the Board on the updates/revisions and secure their support.
2. <i>What are the policy considerations for developing BCPs?</i>	BCPs should be developed in the context of and support existing incident, compliance, risk management, and safety policies.
3. <i>How involved should the Board be in developing and maintaining the BCP?</i>	Board members should assist with providing information, community connections and other supports during the initial development of the BCP. Following the initial development, the board should be kept aware of changes to the plan and rationale, results of training/drills, post-mortem reviews/assessments after disasters, and need for different/additional support.
4. <i>How are BCPs for multi-site health centers different from single-site health centers?</i>	In general, there will be a corporate level BCP that applies to all centers with customizations to the plan for individual health centers.
5. <i>How much does it cost to develop a BCP?</i>	The biggest cost is staff time. When initially developing the plan, it is recommended that the BCP planning group meet regularly with specific tasks assigned between meetings to ensure that there is a regular cadence and time allocated for completing the plan. Additional expenditures may include the cost of an external consultant/contractor to facilitate the plan development.
6. <i>When is the best time to develop a BCP?</i>	It's always a good time to start. Don't wait. Incorporate the lessons and effective strategies learned from managing the health center during the pandemic (e.g., telemedicine, supply chain contingency plans, creative use of outdoor and other spaces, etc.) It's never too late!



CHAPTER 13 | KNOWLEDGE CHECK: INTRODUCTION TO BUSINESS CONTINUITY PLANNING

Check your understanding of some of the major concepts shared in this module. Review sections of the module for which you are unsure of the answers.


QUESTIONS

- BCPs allow health centers to (select the best answer):
 - Maintain or restart operations efficiently
 - Build patient and staff confidence
 - Protect their supply chains
 - Mitigate financial and cybersecurity risk
 - All of the above
- CMS Emergency Preparedness Final Rule § 491.12 requires FQHCs to have a _____ (fill in the blank).
- There is no way to predict what kinds of disasters may impact my health center. True/False
- Business Continuity Plans are best completed during “sunny skies.” True/False
- Power grid failures, employee strikes and pandemics are all classified as human or human-caused disasters. True/False
- Which of the following are NOT major components of comprehensive BCPs? (select all that apply)
 - Executive Summary
 - Hazard Vulnerability Analysis Summary
 - Cybersecurity Impact Analysis Summary
 - Vacation/PTO time analysis
 - Business Impact Analysis Summary
 - Staff personal belongings inventory
 - Leadership Orders of Succession/Delegation of Authority
 - Patient automobiles make, model and license numbers
 - Mitigation plan/strategy for all identified risks
 - Recovery Strategies
 - Implementation Timeline
- Place the following BCP development processes in order from first to last (1-6):
 - Identify types of disasters to be considered in the plan
 - Educate the organization and community
 - Secure senior leaders and Board of Directors’ support for the staff involved in developing the plan and funding for needed resources
 - Identify preparation, mitigation and recovery strategies
 - Conduct vulnerability and impact analyses
 - Designate a BC planning leader, multidisciplinary BCP team, and acknowledge time commitments (e.g., regular schedule of meetings and time to work on the plan)
- The composition of the multidisciplinary BC planning team should be standardized across health centers and include specific health center and department leaders. True/False
- Health Center data are highly desirable targets for cybercriminals. True/False
- Oftentimes when developing a BCP, health centers discover _____ in their normal operations that should be addressed. (select the best answer)
 - Glitches
 - Inefficiencies
 - Dust bunnies
 - Paradoxes
 - Zingers

KNOWLEDGE CHECK ANSWERS

1. E 2. Emergency plan that addresses continuity of operations 3. False 4. True	5. False 6. D, F, H 7. 1-C, 2-F, 3-A, 4-E. 5-D, 6-B	8. False 9. True 10. Inefficiencies
--	---	---

CHAPTER 14 | PREPARING FOR MODULE 2: CREATING THE BUSINESS CONTINUITY PLAN FOR YOUR HEALTH CENTER

OVERVIEW	PREPARING FOR MODULE 2	
<p>The next module is focused on the development of the BCP, including the components of the plan and utilization of the tools and templates provided. Module 2 is appropriate for all health center leaders and board members who have an interest in and/or will be engaged in the BC planning process.</p>		<p>REFLECT ON...</p> <ol style="list-style-type: none"> 1. What are the most compelling reasons <i>my</i> health center should create a BCP? 2. What strengths can the BC planning team draw upon to help develop the plan? 3. How much of the BCP may already be addressed in existing emergency policies and procedures? 4. What areas/components of the BC planning process may require the most time and effort? 5. Will we need to develop a Business Case? 6. What are my other concerns?

APPENDIX A | GLOSSARY OF BUSINESS CONTINUITY PLANNING

Bot/Botnet: A type of software application or script that performs tasks on command, allowing an attacker to take complete control remotely of an affected computer.

Business Continuity: The capability to continue essential business processes under all circumstances.

Business Continuity Planning (BC Planning): An all-encompassing, “umbrella” term used to describe the comprehensive process of planning for the recovery of operations in the event of a disruptive/disaster event.

Business Continuity Plan (BCP): The business continuity plan is a document that defines recovery responsibilities and resources necessary to respond to a disruption to business operations.

Business Impact Analysis (BIA): A review of current operations, with a focus on business and clinical essential services, to determine the effect that a business disruption would have on normal business operations. Impacts are measured in either quantitative or qualitative terms. This information is used to drive the recovery planning process, the potential recovery solutions, and the amount of expenditure required to support the backup of certain business operations. The BIA identifies critical agency functions and supporting technology and support functions necessary to meet the Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

Crisis Communication Plan: a plan developed to share information quickly and accurately with important stakeholders following a disaster or emergency.

Cyber Attack: An act, usually through the Internet, that attempts to undermine confidentiality, integrity, or availability of computers or computer networks, or the information that resides within the systems themselves. A cyber-attack is sometimes referred to as hacking.

Critical Process Essential functions that are important to the mission of the organization and must be maintained during an emergency event.

Cyber Crime: A criminal act involving computers or computer networks. Cybercrimes can be comprised of cyber-attacks such as stalking and distribution of viruses and other malicious code or traditional crimes (e.g., bank fraud, identity theft, and credit card account theft).

Cyber Security Analysis: the process of analyzing potential threats to the security of an organization’s computers, servers, mobile devices, electronic systems, networks, and data from attacks. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common security categories: *Network, Application, Information and Operational*.

Disaster: A sudden, calamitous event that seriously disrupts the functioning of a community or society and causes human, material, and economic losses that exceed the community’s or society’s ability to cope using its own resources.

Disaster (healthcare perspective): Any situation where the incident, numbers of patients, or severity of illness impacts or exceeds the ability of the facility or system to care for them.

Donor MOU Partner The healthcare organization that provides personnel, pharmaceuticals, supplies, or equipment to a facility experiencing a medical disaster.

Donor-Receiving MOU Partner

The healthcare organization that receives transferred patients from a facility responding to a disaster. When personnel or materials are involved, the providing healthcare organization is referred to as the donor healthcare organization.

Emergency: A condition of disaster or of extreme peril to the safety of persons and property caused by natural, technological, or man-made events that may have a quick or slow onset.

Emergency Management Plan (EMP): The plan developed for organizations that identifies how the organization will respond to all disruptions or emergencies. Also called an Emergency Operations Plan (EOP).

Executive Summary: Demonstrates that the Business Continuity Plan is an ongoing process supported by senior management and is funded by the organization. It is usually the introduction to the plan.

Finance/Administrative Section Chief: The Finance/Administration Section Chief is responsible for all financial, administrative, and cost analysis aspects of an incident. The Finance/Administration Section must fiscally manage the incident, including claims processing, contracting, and administrative functions.

Hazard: A hazard is related to the probability that a natural event, or one caused by human activity, may occur in the facility or region; A potential or actual force with the ability to cause loss or harm to humans or property.

Hazard Vulnerability Analysis (HVA): An event-focused, systematic approach to identify, assesses, and prioritize each hazard that may affect a health center. It identifies the health center's vulnerabilities. The vulnerability is related to both the impact on the organizational function and the likely demands created by the hazard impact.

Impacted MOU Partner: The healthcare organization where the disaster occurred or where disaster victims are being treated. Referred to as the Impacted MOU Partner when pharmaceuticals, supplies, or equipment are requested or, as the patient transferring healthcare organizations when the evacuation of patients is required.

Incident Command Center (ICC): An area established in a healthcare organization during an emergency that is the facility's primary source of administrative authority and decision-making.

Incident Commander: The Incident Commander (IC) is responsible for the overall management of the incident. The IC establishes the strategy and tactics for the incident response effort and has the ultimate responsibility for the success of all response and recovery activities. The IC role is filled at every incident, no matter how small or large and is selected by qualifications, experience, and level of authority within the organization. In collaboration with Section Chiefs, the IC determines incident objective and strategy, sets immediate priorities, and authorizes an Incident Action Plan.

Jurisdiction DOC/EOC (Jurisdiction Department Operations Center/Emergency Operations Center): A communication and information center that has MAS network capabilities allowing for the immediate determination of available healthcare organizations resources at the time of a disaster. The Jurisdiction DOC/EOC does not have any decision-making or supervisory authority and merely collects and disseminates information.

Liaison Officer: The Liaison Officer's (LO) role is to serve as the point of contact for assisting and coordinating activities between the Incident Commander and other healthcare providers and government agencies. The LO reports directly to the Incident Commander.

Logistics Section Chief: The Logistics Section Chief manages logistical needs and provides facilities, services, people, and materials in support of the incident. The Logistics Section is responsible for all service support requirements needed to facilitate effective and efficient incident management, including ordering resources from off-incident locations. This Section also provides facilities, security, transportation, supplies, equipment maintenance and fuel, food services, and communications and information technology support.

Malware: An umbrella term that describes all forms of malicious software designed to wreak havoc on a computer. Common forms include viruses, trojans, worms and ransomware.

Medical Disaster: An incident that exceeds a facility's effective response capability or a situation that cannot be appropriately resolved solely by using the facility's own resources. Such disasters will very likely involve the local emergency management agency, Jurisdiction Emergency Management Agency, the Jurisdiction Public Health Department and may involve the mobilization of publicly owned response materials and equipment or the loan of medical and support personnel, pharmaceuticals, supplies, and equipment from another facility, or, the emergent evacuation of patients.

MAS: Mutual Aid System

Operations Section Chief: The Operations Section Chief manages the incident's tactical operations by directly supervising all resources assigned to the Operations Section. The function of the Operations Section is to accomplish the response and recovery strategies by directing resources to execute tactical objectives. The Operations Section Chief directs all the incident tactical operations and assists the IMT in the development of the Incident Action Plan (IAP).

Participating healthcare organizations: Health care facilities that have fully committed to MAS and signed the healthcare organization Memorandum of Understanding.

Partner (“Buddy”): The designated facility that an Impacted healthcare organization communicates with as a facility’s “first call for help” during a medical disaster (developed through an optional partnering arrangement). MOU Partner should meet at least twice a year to discuss contingency plans.

Phishing or Spear Phishing: A technique used by hackers to obtain sensitive information. Such as using email messages designed to trick people into divulging personal or confidential data such as passwords and bank account information.

Planning Section Chief: The Planning Section Chief supervises the collection, evaluation, processing, and dissemination of the Incident Action Plan (IAP). The function of the Planning Section is to collect and evaluate information that is needed for preparation of the IAP. The Planning Section forecasts the probable course of events the incident may take and prepares alternative strategies for changes in or modifications to the IAP.

Process: A systematic series of activities or tasks that produce a specific end.

Public Information Officer: The Public Information Officer (PIO) reports to the Incident Commander and is responsible for the development and release of information about the incident. The PIO conducts media briefings, develops messaging, distributes information to incident personnel and works closely with other members of the IMT.

Ransomware: A form of malware that deliberately prevents you from accessing files on your computer – holding your data hostage. It will typically encrypt files and request that a ransom be paid to have them decrypted or recovered.

Recipient healthcare organization: The impacted facility. The healthcare organization where disaster patients are being treated and have requested personnel or materials from another facility.

Recovery Point Objective (RPO): The point in time to which data must be restored in order to resume processing transactions. RPO is the basis on which a data projection strategy is developed.

Recovery Time Objective (RTO): The time it takes to restore data and system/application functionality that must be restored in order to resume processing transactions.

Risk: A risk is related to the probability, based on history, that certain identified hazards will occur. These circumstances are closely related not only history and to the level of exposure and impact of an event, but to the vulnerability to the effects of the event. The effect of hazard combined with vulnerability.

Safety Officer: The Safety Officer is responsible for monitoring and assessing hazardous and unsafe situations as well as developing measures for assuring personal safety. The Safety Officer reports directly to the IC and is the only person that can supersede the IC in the event of an unsafe situation.

Staff (or personnel): Staff or personnel are employees of a specific healthcare organization.

Spyware: A type of malware that functions by spying on user activity without their knowledge.

Trojan Horse: A piece of malware that often allows a hacker to gain remote access to a computer through a “back door”.

Virus: A type of malware aimed to corrupt, erase, or modify information on a computer before spreading to others. However, in more recent years, viruses like Stuxnet have caused physical damage.

Vulnerability: How susceptible resources are to the negative effects of hazards including the likelihood of a hazard occurring, and the mitigation measures taken to lessen the effects of hazards.

Worm: A piece of malware that can replicate itself in order to spread the infection to other connected computers.

For a more extensive glossary check: [FEMA’s Glossary of Terms](#)

APPENDIX B | BUSINESS CONTINUITY PLANNING RESOURCES TOOLBOX

Hint: Use key word search to find resources (CTRL + F)



1. Business Case for Remote Work – For Employers, Employees, the Environment, and Society Design Public Group and Global Workplace Analytics. 2021. <https://globalworkplaceanalytics.com/download/235613/>
2. Business Continuity Business Case Template. Castellan. Note: Email address and job title are required to download this resource. <https://castellanbc.com/template/business-continuity-business-case/#form>
3. [Business Continuity Plan Example A](#). NACHC.
4. [Business Continuity Plan Example B](#). NACHC.
5. Business Continuity Planning Institute Webinar Series. NACHC. 2021.
 - a. Introduction to Business Continuity Planning webinar PowerPoint presentation, NACHC, 2021. <https://protect-us.mimecast.com/s/mK89COY2DylkwkmtrsasZ> Webinar: <https://www.youtube.com/watch?v=NVhrCTCMLm4>
 - b. Creating a Business Continuity Plan webinar PowerPoint presentation, NACHC, 2021. <https://protect-us.mimecast.com/s/orGJCQW2G0sL9LjuAYV7D> Webinar: <https://www.youtube.com/watch?v=zduGYCeQTnE>
 - c. Ensuring a Human Resource Strategy Webinar PowerPoint presentation, NACHC, 2021. <https://protect-us.mimecast.com/s/TWSpCVOKjPu8X8oTEVuh4> Webinar: <https://www.youtube.com/watch?v=yO3BABszjJc>
6. Business Continuity Planning Interactive Learning Series. NACHC. 2022.
 - a. Introduction to Business Continuity Planning
 - b. Creating a Business Continuity Plan
 - c. Ensuring a Human Resource Strategy
7. Business Continuity Planning Suite. FEMA. <https://www.ready.gov/business-continuity-planning-suite>
8. Business Continuity Planning Suite. Business Continuity Training Part 2: Why is Business Continuity Planning Important? FEMA. <https://www.youtube.com/watch?v=PDW4luQneeQ>
9. Business Impact Analysis. 2021. Ready.gov: <https://www.ready.gov/business-impact-analysis>
10. Business Continuity Training Introduction (video). Ready.gov. https://www.youtube.com/watch?v=R1oIQ4Y_EHY&list=PL720Kw_OoJlly2uSz0VTHM-Whk-Su8Ucy&index=1
11. CMS Emergency Preparedness Final Rule Updates - Rural Health Clinic / Federally Qualified Health Center Requirements, Effective March 26, 2021. <https://files.asprtracie.hhs.gov/documents/aspr-tracie-cms-ep-rule-rhc-fqhc-requirements.pdf>
12. Common Disasters Across the U.S. American Red Cross. <https://www.redcross.org/get-help/how-to-prepare-for-emergencies/common-natural-disasters-across-us.html#all>
13. Continuity Plan Template and Instructions for Non-Federal Entities and Community Based Organizations. FEMA, August 2018. https://www.fema.gov/sites/default/files/2020-10/non-federal-continuity-plan-template_083118.pdf
14. COVID-19 Response Resources. NACHC. <https://www.nachc.org/clinical-matters/current-projects/building-capacity-of-community-health-centers-to-respond-to-covid-19/>
15. Creating a Business Continuity Plan For Your Health Center, May 2021. NACHC. https://www.nachc.org/wp-content/uploads/2020/11/Business-Continuity-Manual_Interactive-1.pdf
16. Crisis & Emergency Risk Communication (CERC). CDC. January 23, 2018. <https://emergency.cdc.gov/cerc/>
17. Cybersecurity. Ready.gov. 11/18/2020. <https://www.ready.gov/cybersecurity>
18. Cybersecurity in Healthcare. Healthcare Information and Management Systems Society (HIMSS). The Healthcare Information and Management Systems Society (HIMSS) discusses the three goals of cybersecurity: protecting the confidentiality, integrity and availability of information, also known as the “CIA triad.” <https://www.himss.org/resources/cybersecurity-healthcare>
19. Disaster Declarations for States and Counties. FEMA. Explore historic federal disaster declarations by state, county, hazard, and year. <https://www.fema.gov/data-visualization/disaster-declarations-states-and-counties>
20. [Employee Assistance & Support](#). Ready.gov. 2/17/2021
21. Engaging in Succession Planning. Society for Human Resource Management (SHRM). 2017. Detailed overview of succession planning, rationale, methods, and business case. May be most appropriate for HR professionals. <https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/engaginginsuccessionplanning.aspx>
22. Federal Labor Laws. U. S. Department of Labor. <https://www.dol.gov/general/aboutdol/majorlaws>
23. Glossary of Terms. FEMA. <https://www.fema.gov/pdf/plan/glo.pdf>
24. Good Samaritan Hospital: Business Continuity Guide for Critical Business Areas (PDF, Sample/Template). <https://www.calhospitalprepare.org/sites/main/files/file-attachments/goodsam.pdf>
25. Guide to Developing an Effective Business Continuity Plan. 2020. Noggin. <https://www.noggin.io/hubfs/Noggin%20-%20Guide%20to%20Effective%20BCP%20-%20December%202020.pdf>
26. Hazard Information Sheets Suite. FEMA. https://www.ready.gov/sites/default/files/2021-01/ready_full-suite_hazard-info-sheets.pdf

27. Healthcare Business Continuity Management and Disaster Recovery— No Longer an Afterthought in Today's World. 2019. Association of Healthcare Internal Auditors (AHIA) and Crowe. <https://ahia.org/getattachment/news/White-Papers/AHIA-Crowe-Whitepaper.pdf?lang=en-US>
28. HIT Solution for Clinical Care and Disaster Planning: How One Health Center in Joplin, MO Survived a Tornado and Avoided a Health Information Disaster. (Shin P, Jacobs F.) Online J Public Health Inform. 2012;4(1):ojphi.v4i1.3818. doi: 10.5210/ojphi.v4i1.3818. Epub 2012 May 17. PMID: 23569622; PMCID: PMC3615799. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3615799/>
29. Hospital Continuity Planning Toolkit. 2012. California Hospital Association Hospital Preparedness Program Hospital Continuity Planning Workgroup. https://www.calhospitalprepare.org/sites/main/files/file-attachments/hcp_toolkit_1.pdf
30. Hospital Incident Command System, Internal Scenarios. 2006. Emergency Management Services Authority of California. <https://emsa.ca.gov/hospital-incident-command-system-internal-scenarios/>
31. Hospital Incident Command System, External Scenarios. 2006. Emergency Management Services Authority of California. <https://emsa.ca.gov/hospital-incident-command-system-external-scenarios/>
32. How to Make a Business Case. Workfront.com. Template for making a business case. <https://www.workfront.com/project-management/life-cycle/initiation/business-case>
33. Incident Management. Ready.gov. 5/26/2021. <https://www.ready.gov/incident-management>
34. Interactive Disaster Map. The Ready Store. Learn the likelihood of specific natural disasters affecting your state. <https://www.thereadystore.com/natural-disaster-map/>
35. Joint Commission Emergency Management Requirements. https://store.jcrinc.com/assets/1/7/cc_hap_em.pdf
36. PrepTalks. FEMA. 33 presentations by subject-matter experts and thought leaders to spread new ideas, spark conversation, and promote innovative leadership for the issues confronting emergency managers now and over the next 20 years. https://www.youtube.com/playlist?list=PL720Kw_OoJlJiYKDZQwKG7HAgV_qNjblB
37. ReadyBusiness Toolkit. FEMA. The Ready Business Toolkit series includes hazard-specific versions for earthquake, hurricane, inland flooding, power outage, and severe wind/tornado. Toolkits offer business leaders a step-by-step guide to build preparedness within an organization. Each toolkit contains the following sections: Identify Your Risk; Develop A Plan; Take Action; Be Recognized and Inspire Others. <https://www.ready.gov/business>
38. Rural Health Clinic / Federally Qualified Health Center Requirements CMS Emergency Preparedness Final Rule Updates Effective March 26, 2021. <https://files.asprtracie.hhs.gov/documents/aspr-tracie-cms-ep-rule-rhc-fqhc-requirements.pdf>
39. State Labor Laws, U. S. Department of Labor. <https://www.dol.gov/agencies/whd/state>
40. State of Remote Work 2021. Owl Labs and Global Workplace Analytics. <https://globalworkplaceanalytics.com/download/239489/>
41. Succession Planning: A Step-By-Step Guide. NIH, Office of HR. 2021. <https://hr.nih.gov/sites/default/files/public/documents/2021-03/Succession Planning Step by Step Guide.pdf>
42. Telecommuting. TechTarget.com. Overview of telecommuting pros, cons, and the business case. <https://www.techtarget.com/searchmobilecomputing/definition/telecommuting>
43. Telecommuting Policy and Procedure Sample. Society for Human Resources Management (SHRM). https://www.shrm.org/resourcesandtools/tools-and-samples/policies/pages/telecommuting_policy.aspx
44. Two Types of Succession Plans and Why Your Company Needs Both. RCLCO, Real Estate Consulting. November 14, 2019. <https://www.rclco.com/wp-content/uploads/2019/11/The-Two-Types-of-Succession-Plans-and-Why-Your-Company-Needs-Both.pdf>
45. Types of Disasters. SAMHSA. <https://www.samhsa.gov/find-help/disaster-distress-helpline/disaster-types>
46. Wakefield- Brunswick. Santa Cruz County Business Continuity Plan Example (template). <https://www.santacruzhealth.org/Portals/7/Pdfs/HPP/CO LTC SNF Template.docx>
47. What is Succession Planning? 7 Steps to Success. Robert Half. 10/3/2021. Here are seven tips for kick-starting the succession planning process at your company. <https://www.roberthalf.com/blog/management-tips/7-steps-to-building-a-succession-plan-for-success>
48. What's a Business Continuity Plan? FEMA. Ready.gov video available on YouTube. https://www.youtube.com/watch?v=R1oIQ4Y_EHY&list=PL720Kw_OoJlly2uSz0VTHM-Whk-Su8Ucy&index=1
49. Yale Guide to Business Continuity and Recovery Planning – General. 2016. Yale Office of Emergency Management. <https://emergency.yale.edu/sites/default/files/files/Guide-BCP-General-Audience.pdf>