BUSINESS CONTINUITY PLANNING FOR IMMUNIZATION INFORMATION SYSTEM PROGRAMS

RECOMMENDATIONS OF THE AIRA MODELING OF IMMUNIZATION REGISTRY OPERATIONS WORKGROUP (MIROW)

DECEMBER 2019

AIRA
AMERICAN IMMUNIZATION REGISTRY ASSOCIATION

Developing a business continuity plan and a system to manage business continuity allows an IIS program to better respond to disruptions and recover quickly.

EXECUTIVE SUMMARY

BACKGROUND

> When is an alternative process implemented if normal immunization information system (IIS) functionality is not working? Who is informed when the IIS user interface (UI) is unavailable to users?

Most IIS programs have dealt with disruptions to their services. These disruptions can range from small issues, like a report not being available to run for a few hours, to large problems, like losing complete IIS functionality for days. These experiences have led to an interest from the IIS community in learning more about how to manage disruptions.

"Business continuity" is a term used to describe "the strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions to continue business operations at an acceptable predefined level."[1] Developing a business continuity plan and a system to manage business continuity allows an IIS program to better respond to disruptions and recover quickly. This guide walks jurisdictions through the process of developing a business continuity plan that can be used during a disruption and the additional pieces that are important to ensure the concepts of the plan are integrated into the IIS program.

KEY RECOMMENDATIONS

- Involve stakeholders during the development process.
- Follow the steps in the business continuity plan development process to create a business continuity plan.
- Use the business continuity plan to prepare to:
  - Prevent or mitigate the risk of disruptions
  - Continue operations in the event of a disruption
  - Recover to normal operations after a disruption
- Educate and train staff about the business continuity plan.
- Exercise the business continuity plan.
- Ensure resources are available to support the development of the business continuity plan and to support post-planning activities.

[1] ISO 22313:2012(E), *Societal security — Business continuity management systems — Guidance*

IMPLEMENTATION

The recommendations in this document attempt to balance ideal practices with pragmatic considerations of what is possible to implement in an IIS. Specific implementation may vary based on resources, goals, needs, and unique jurisdictional concerns of each IIS. The recommendations presented here may be adopted incrementally and are not exhaustive. Finally, the recommendations are not static—they will need to change and evolve over time as business requirements change.

This guide is intended to help with the development and implementation of business continuity plans.

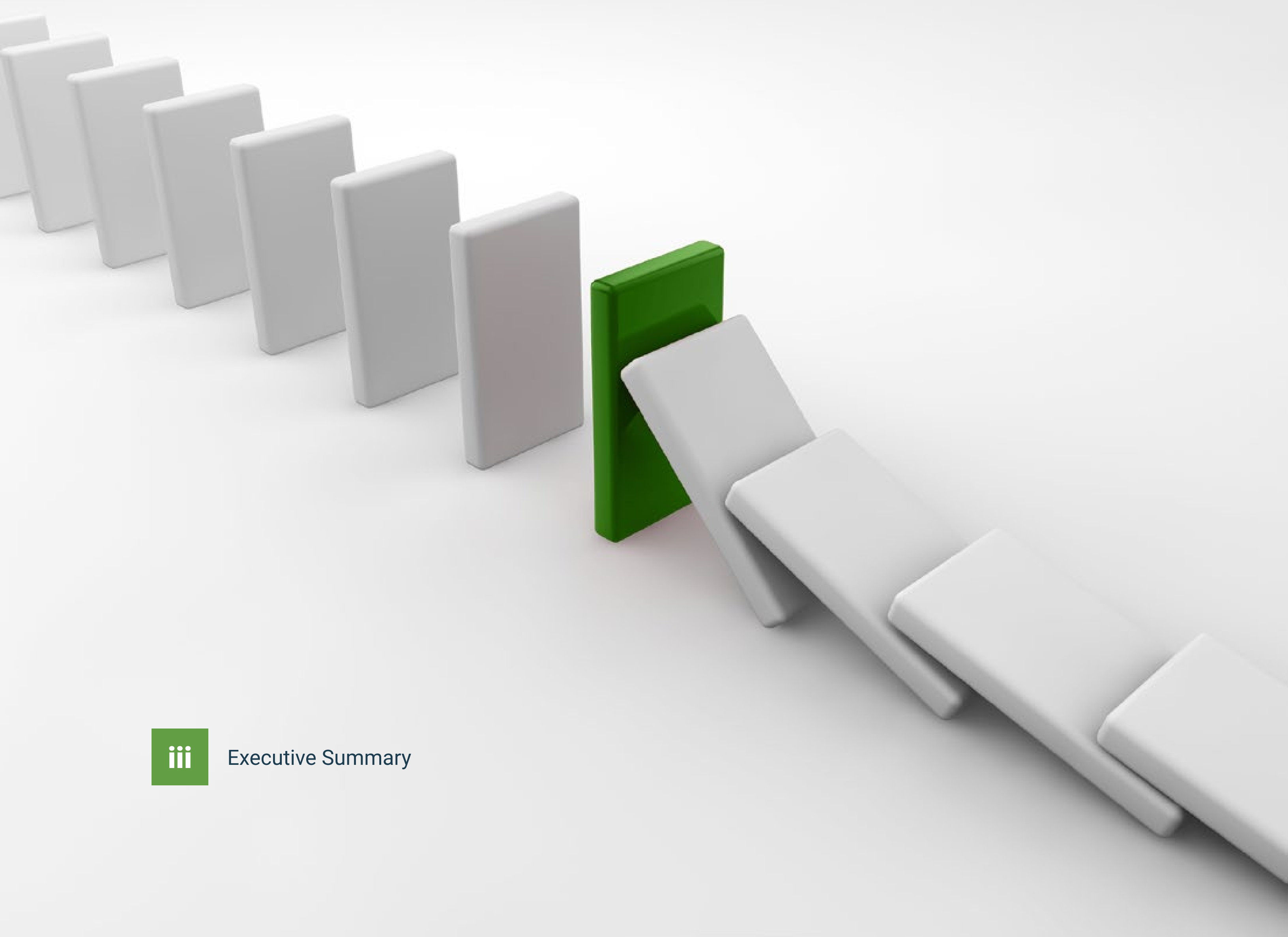


TABLE OF CONTENTS

APPENDICES

APPENDICES

1

INTRODUCTION

Business continuity is an organization's ability to manage and respond to disruptions in an organized and effective manner.

1 INTRODUCTION

1.1 BACKGROUND

Many immunization information system (IIS) programs have experienced some type of disruption. These disruptions can be caused by events ranging from hurricanes to staff illness.

Building an IIS program's business continuity capacity reduces the risk of disruptions and decreases the time required to resume operations. Business continuity is an organization's ability to manage and respond to disruptions in an organized and effective manner.

Developing a business continuity plan and a system to manage business continuity offers several important benefits:

- **Improved management of disruptions and speedy recovery**
- **Better understanding of the IIS program's operations and processes**
- **Sustained institutional knowledge about business continuity for the IIS program**

This guide aims to help with the development and implementation of business continuity plans.

1.2 HIGHLIGHTS OF THIS GUIDE

- Overview of the key concepts related to business continuity (Chapter 2)
- A step-by-step process for developing a business continuity plan (Chapter 3)
- Discussion of implementation considerations, including:
  - Business continuity planning process in a context of broader concepts and initiatives (Chapter 4)
  - Post-planning activities (Chapter 5)
  - Use of the business continuity plan during a disruption (Chapter 6)
- A list of principles to guide the development and use of a business continuity plan (Chapter 7)
- Tools and examples to support the creation and use of a business continuity plan (Appendices)

1.3 TARGET AUDIENCE

This entire guide is designed to be read by ground-level staff that will develop and implement a business continuity plan. Immunization and IIS program leadership should read the executive summary and the mini-guide.[2] This guide may also be helpful to other public health programs interested in business continuity.

1.4 INTENDED USE

This guide contains recommended best practices presented in a form of the suggested process for developing and implementing a business continuity plan for an IIS program. Modeling of Immunization Registry Operations Workgroup (MIROW) best practice recommendations are independent from specific IIS implementations and technology solutions. The implementation of these best practice recommendations will vary based on the specific IIS. Resource constraints may also lead to partial or incremental adoption of these guidelines. The IIS program can also use this guide for staff training and communication purposes.

[2] https://repository.immregistries.org/resource/business-continuity-planning-for-immunization-information-system-programs

1.5 SCOPE

The scope includes recommendations for IIS programs to develop and implement a business continuity plan for selected essential business functions that are supported by the IIS. The focus is on sustaining continuous business operations as opposed to sustaining information technology (IT) systems that support those business operations. The essence of development for this topic is application of an established business continuity framework for essential business functions identified by the IIS program. The guide includes recommendations for:

- Initiation of a business continuity planning process
- Assessment of threats for the organization overall
- Business impact analysis:
    - Examining business functions and the effect that a disruption might have upon them
    - Identifying essential business functions and associated resources
    - Determining important time frames
- Risk assessment: examining the level of risk that exists for a specific resource needed to support a selected essential business function
- Risk mitigation strategies and business continuity options for essential business functions identified by the IIS program
- Communication related to developing and implementing a business continuity plan
- Education and training for a business continuity plan and exercise (i.e., testing) of a business continuity plan
- Review and update of a business continuity plan
- Plan activation, standing down, and resumption of normal activities

Appendix C includes a more detailed description of the scope.

1.6 ABOUT MIROW

The American Immunization Registry Association (AIRA), in partnership with the National Center for Immunization and Respiratory Diseases at the Centers for Disease Control and Prevention (CDC), formed MIROW to develop best practice guidance for IIS. Since 2005, MIROW has developed several guides for IIS functional areas. For more information about MIROW and the development process for MIROW guides, see the *MIROW and the Best Practice Development Process* document. Subject matter experts who contributed to this document represent a variety of IIS programs. All contributors are listed in Appendix V.

2

FUNDAMENTAL CONCEPTS

As a broad concept, business continuity is an organization’s ability to manage and respond to disruptions in an organized and effective manner.

2 FUNDAMENTAL CONCEPTS

> Business continuity is defined as “the strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions to continue business operations at an acceptable predefined level.”[3]

As a broad concept, business continuity is an organization’s ability to manage and respond to disruptions in an organized and effective manner. The idea of business continuity is actualized by developing and implementing a business continuity plan and a business continuity management system.

A BUSINESS CONTINUITY PLAN includes the documented procedures that guide organizations to mitigate the impact of a disruption and to respond, recover, resume, and restore to a predefined level of operation following disruption.[4]

A BUSINESS CONTINUITY MANAGEMENT SYSTEM is “a part of an overall management system that establishes, implements, operates, monitors, reviews, maintains, and improves business continuity.”[5]

Simply put, a business continuity management system helps an organization integrate the business continuity plan into its regular operations and ensures that the plan is regularly exercised and updated.

Business continuity is an important element in developing a sustainable organization or program. For this reason, business continuity plans and management systems have been implemented in a wide variety of businesses and organizations, and there is a large existing field of knowledge about this topic. Based on business continuity standards, there are certain concepts and processes that are broadly applied to develop a business continuity plan and management system.

The key concepts used in the process of developing and sustaining a business continuity plan are explained in this section. For a more comprehensive set of concepts and associated terms and definitions, refer to Appendix D.

[3] ISO 22313:2012(E), *Societal security — Business continuity management systems — Guidance*
[4] Adapted from ISO 22313:2012(E), *Societal security — Business continuity management systems — Guidance*
[5] ISO 22313:2012(E), *Societal security — Business continuity management systems — Guidance*

2.1 IIS BUSINESS CONTINUITY PLAN VS. OTHER PLANS

The focus of a business continuity plan is on managing the impact of losing access to a resource due to a disruption.

- **Resources:** "The people, information and data, technology, buildings/worksites, communication systems, equipment, and utilities that an organization has to have available to operate."[6] While information, data, and technology can be resources needed to make business functions work, the focus of this guide is on sustaining continuous business operations as opposed to sustaining IT systems.
- **Disruption:** "An interruption of normal business operations or processes that can range from short-term to longer-term unavailability."[7]

The focus of a business continuity plan is on managing the impact of losing access to a resource due to a disruption.

The business continuity planning process will help an IIS program prepare to respond to losing IIS functionality regardless of the reason for the disruption. Having a business continuity plan will help an IIS program navigate the loss of resources and associated essential business functions due to a disaster but will not address additional functionality needed to respond to a disaster (e.g., ability to collect information about adjuvants in a pandemic).

There are many types of plans that support an organization in terms of security, continuity, preparedness, and recovery. Likewise, different terminology can be used to describe similar types of plans. For example, government organizations often refer to business continuity plans as continuity of operations plans (COOP). A list of types of plans is presented in Appendix E. For more information about how an IIS business continuity plan can integrate with other plans, read Integration into other state and agency plans in Chapter 4.

[6] Adapted from ISO 22313:2012(E), *Societal security — Business continuity management systems — Guidance*
[7] BCM Institute. Disruption. (2015, December 27). Retrieved March 27, 2019, from http://www.bcmpedia.org/wiki/Disruption

“A goal without a plan is just a wish.”

— Antoine de Saint-Exupéry

2.2 BIG-PICTURE CONCEPTS

VALUE OF THE PLAN

Developing a business continuity plan is an important step in supporting the stability of an IIS program. A continuity plan provides a one-stop shop for information when a disruption occurs. Creating and sustaining a business continuity plan demonstrates to staff, leadership, partners, and users that the IIS program is dedicated to ensuring the availability of IIS services and products. A business continuity plan can also help justify actions performed and resources needed during a disruption.

> **A continuity plan provides a one-stop shop for information when a disruption occurs.**

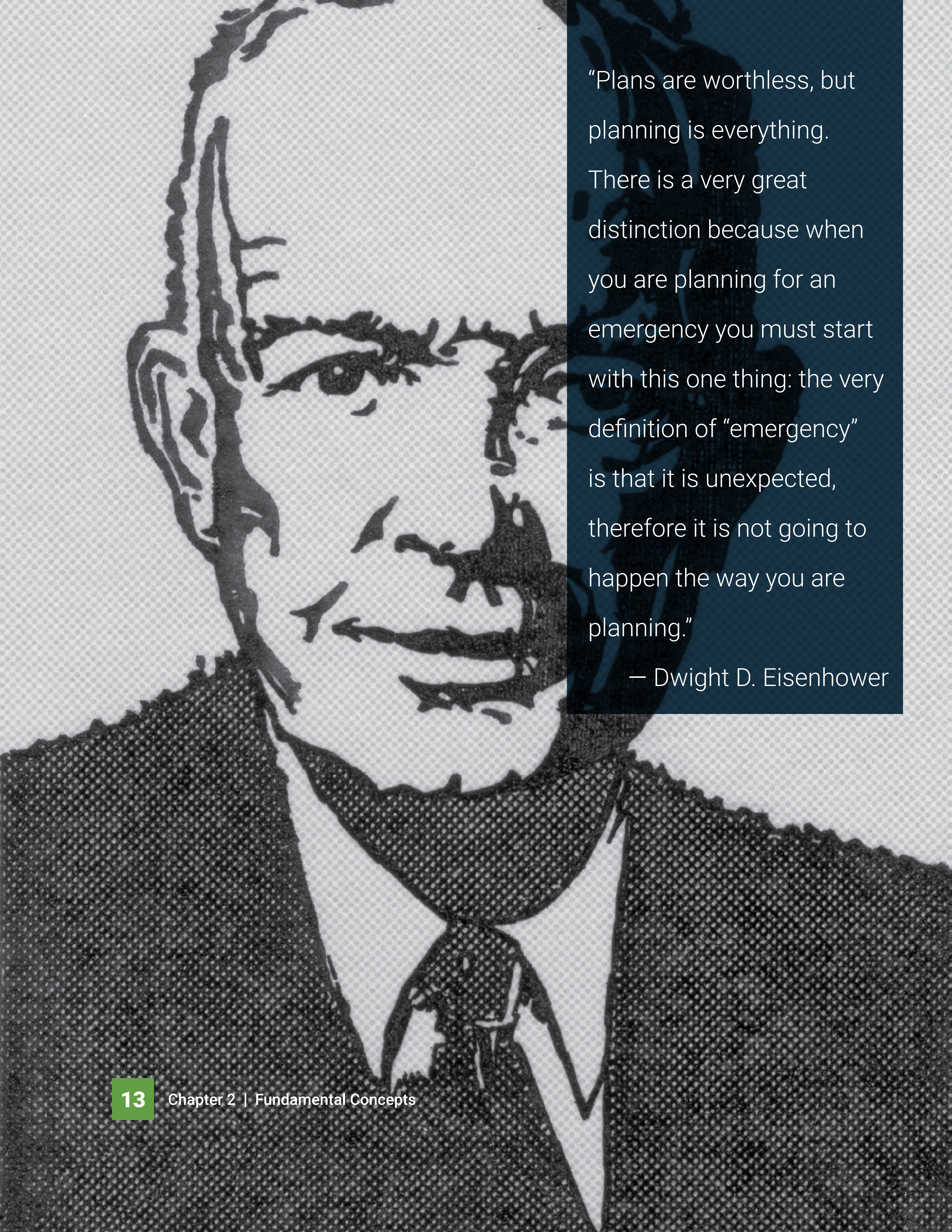
VALUE OF THE PLANNING

No plan can address every possible situation, but that is not a good reason to avoid planning. The process of developing and supporting a business continuity plan offers several important benefits:

- Better understanding of the IIS program's operations and processes
- Increased attention to risks that can impact resources needed for essential business functions supported by an IIS
- Development of staff who can plan and respond to disruptions
- Sustained institutional knowledge about business continuity for the IIS program

VALUE OF THE SYSTEM

Creating a business continuity plan is a valuable process; however, a plan that sits in a file cabinet is not especially helpful. Development of and ongoing support for a business continuity management system will allow for education and training about the plan, exercises of the plan, and will promote making regular updates to the plan. It is crucial to gain support from leadership from the beginning of the process to ensure that the organization provides the ongoing resources needed for a sustainable business continuity management system.



> “Plans are worthless, but planning is everything. There is a very great distinction because when you are planning for an emergency you must start with this one thing: the very definition of “emergency” is that it is unexpected, therefore it is not going to happen the way you are planning.”
>
> — Dwight D. Eisenhower

2.3 PLANNING ACTIVITIES: CONCEPTS FOR DEVELOPING A BUSINESS CONTINUITY PLAN

To develop a business continuity plan, an organization needs to understand which of its products and services are the highest priority and what risks could impact those products and services. Once an organization has this information, staff can develop plans to decrease or remove risks for disruptions and, when a disruption happens, continue to provide (or rapidly resume the provision of) priority products and services. The following section provides an overview of the terminology and concepts that are valuable for understanding the process of business continuity planning. The process is described in detail in Chapter 3, and broader concepts related to developing a business continuity plan are discussed in Chapter 4.

To develop a business continuity plan, an organization needs to understand which of its products and services are the highest priority and what risks could impact those products and services.

WHAT AND WHEN: BUSINESS FUNCTIONS, BUSINESS IMPACT ANALYSIS, AND TIME FRAMES

A business continuity plan should largely focus on preparing for disruptions to the most significant products/services. Products or services are referred to as “business functions.”

- **Business function:** “A description of work that is performed to accomplish a business unit’s responsibility”[8]

The highest priorities or most significant business functions of an organization are referred to as “essential business functions.”

- **Essential business function:** A business function that supports an IIS program’s key products and services and, when interrupted, has significant negative impact on the well-being of the public and IIS staff, IIS reputation, product or service quality, or the ability to meet legal and regulatory requirements

An IIS program should perform a business impact analysis to identify essential business functions.

- **Business impact analysis:** The process of analyzing business functions and the effect that a disruption might have upon them”[9]

[8] BCM Institute. Business Function. (2017, August 28). Retrieved March 27, 2019, from http://www.bcmpedia.org/wiki/Business_Function

[9] Adapted from ISO 22313:2012(E), *Societal security — Business continuity management systems — Guidance*

A business impact analysis supports the step-by-step process to determine which business functions exist; what subset of business functions are potentially essential business functions; and, ultimately, which essential business functions are selected for the continuity plan.

Business impact analysis also helps determine the important time frames related to business continuity.

- **Recovery point objective (RPO):** The point prior to a disruption to which information used by a business function must be restored to minimize the loss of data resulting from the disruption
- **Recovery time objective (RTO):** "The period of time following a disruption within which a business function must be resumed"[10]
  - Resumption of the business function can be by an alternate process (i.e., a workaround) or through restarting normal operations.
- **Maximum tolerable period of disruption (MTPD):** "The time it would take for adverse impacts, which might arise as a result of not providing a business function, to become unacceptable"[11]
  - Like RTO, resumption of the business function can be achieved by an alternate process or through restarting normal operations.

A diagram of the relationship between these three time frames is available in Step 3.4.2 in Chapter 3.

It is recommended that IIS programs use business impact analysis to determine RPO and RTO. MTPD may be useful for certain IIS programs and/or for certain essential business functions.

In short, business impact analysis helps answer the questions, "what are the essential business functions" and "when do these functions need to be resumed."

In short, business impact analysis helps answer the questions, "what are the essential business functions" and "when do these functions need to be resumed."

[10] Adapted from ISO 22313:2012(E), *Societal security — Business continuity management systems — Guidance*
[11] Adapted from ISO 22313:2012(E), *Societal security — Business continuity management systems — Guidance*

WHY: THREAT ASSESSMENT AND RISK ASSESSMENT

An IIS program should also be aware of threats and risks to its essential business functions.

- **Threat assessment:** "An evaluation and description of the type, scope, and nature of events or actions that can result in adverse consequences to an organization or specific assets"[12]
- **Risk assessment:** "An overall process of risk identification, risk analysis, and risk evaluation"[13]

Threat assessments generally look at the impact of major events like fires, natural disasters, or pandemics. The process proposed in this guide involves a very limited amount of threat assessment because this work is commonly done at a higher organizational level (e.g., the state health department).[14,15,16]

Risk assessment looks at the level of risk that exists for a specific resource needed to support an essential business function. For example, the vaccine ordering process requires that ordering staff process orders via the IIS, so a risk assessment evaluates the risk that the IIS would not be available to support vaccine ordering. Risk is calculated by combining the probability and the impact of the resource not being available. Examples of this calculation are included in Task 4 in Chapter 3.

A threat assessment and risk assessment help answer the question, "why might a business function be disrupted."

[12] The Office of Enterprise Technology, State of Minnesota, Glossary of Information Security Terms and Definitions, 2014-08-20. https://mn.gov/mnit/images/SEC_R_Glossary.pdf

[13] ISO 22313:2012(E), *Societal security — Business continuity management systems — Guidance*

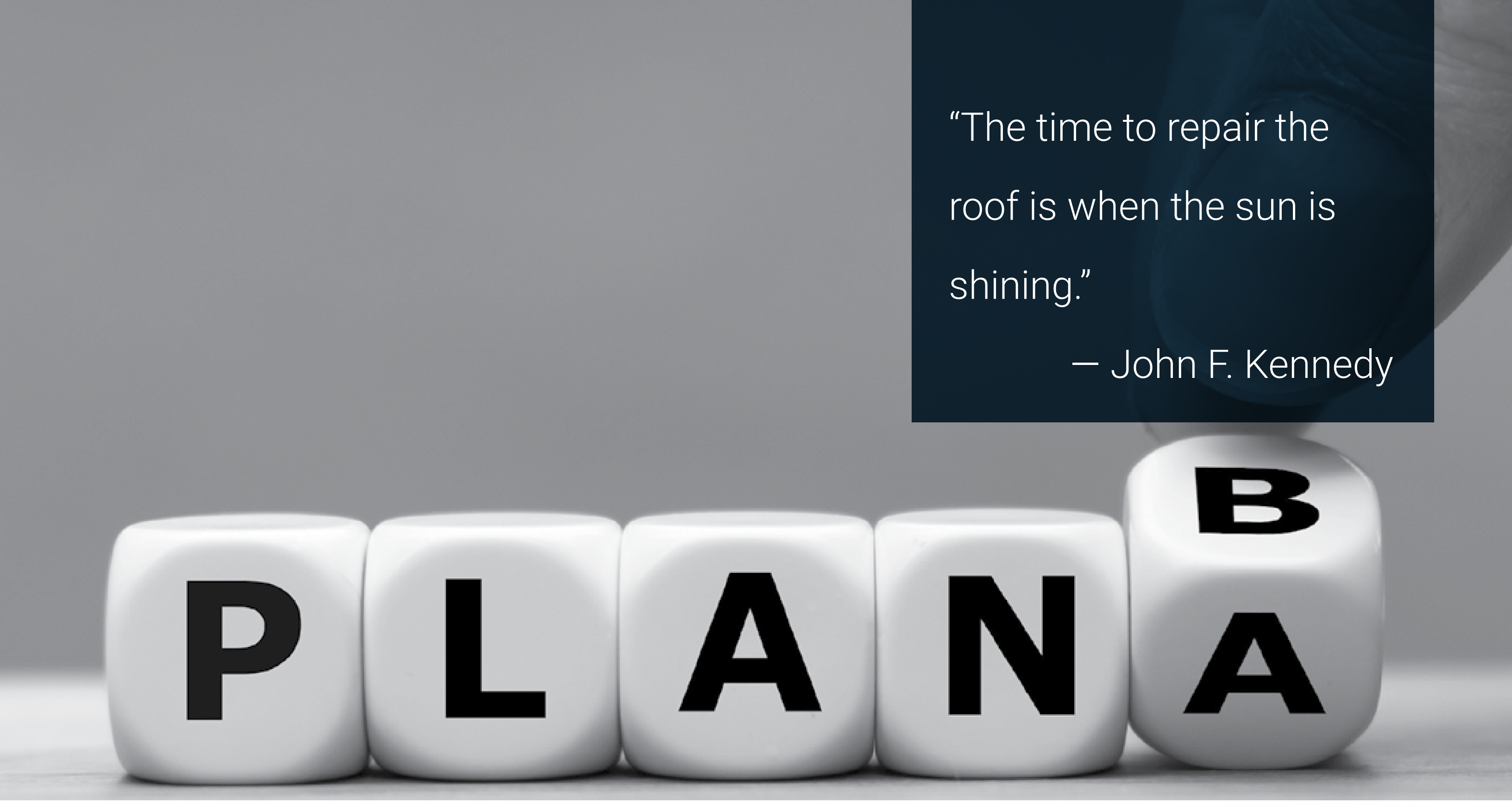
[14] Business Continuity Institute. Good practice guidelines 2013: A Guide to Global Good Practice in Business Continuity. 2013, pp. 57–59.

[15] National Fire Protection Association. *National Fire Protection Association 1600 Standard on Continuity, Emergency, and Crisis Management.* 2019, section 5.2. https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1600

[16] International Organization for Standardization. ISO 22313:2012(E). Societal security — Business continuity management systems — Guidance. 2012. https://www.iso.org/standard/50050.html

“It does not do to leave a live dragon out of your calculations if you live near him.”

— J.R.R. Tolkien



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

— John F. Kennedy

HOW: RISK MITIGATION STRATEGIES AND BUSINESS CONTINUITY OPTIONS

Once the essential business functions and the risks to these functions are identified, the next step is to develop risk mitigation strategies and business continuity options.

- **Risk mitigation:** "To implement measures so as to lower the exposure to risk and lower the probability or impact of a risk"[17]
- **Continuity option:** An alternative course of action, such as using an alternative process or relocation, for implementing a business function affected by a disruption

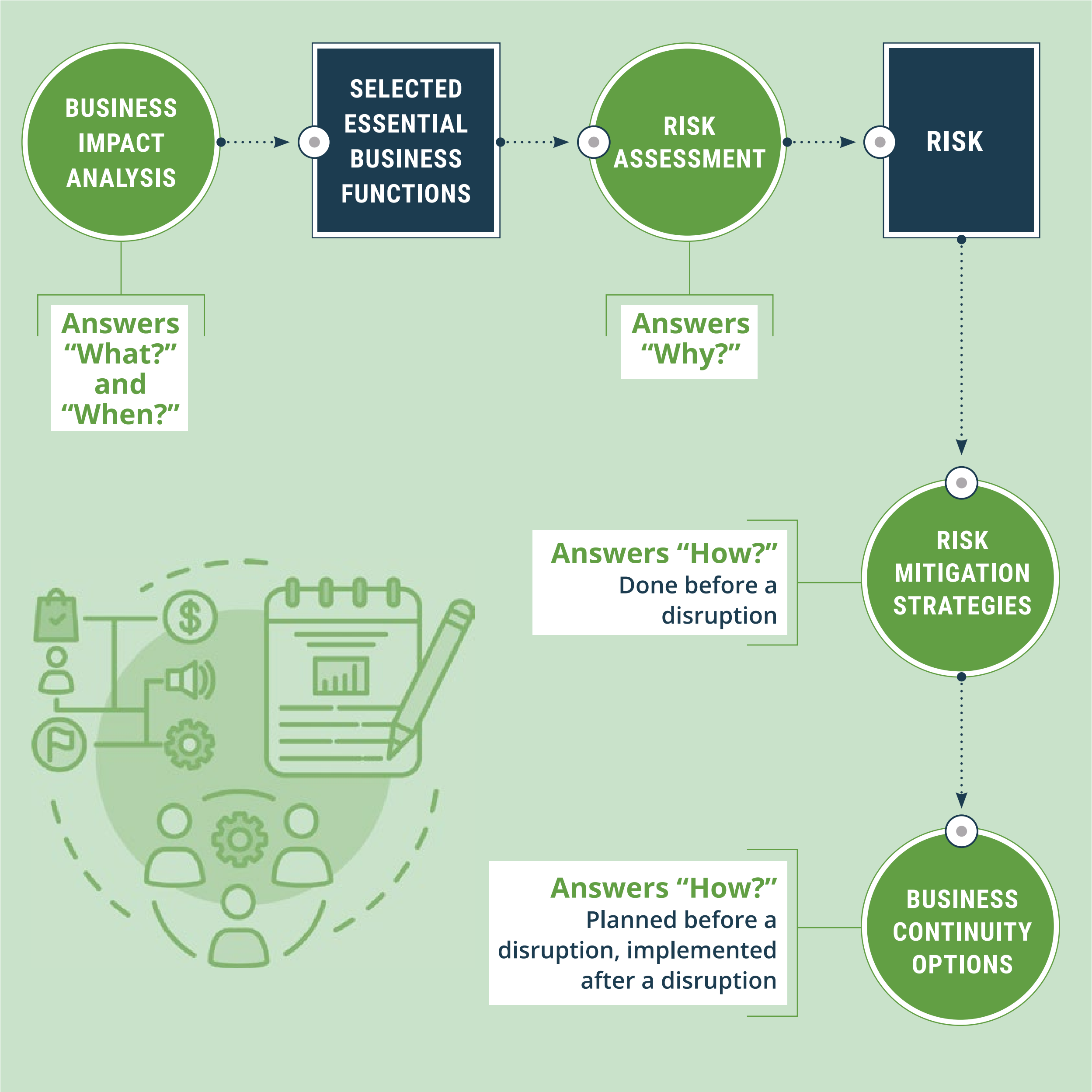
Risk mitigation strategies are planned and implemented before a disruption to decrease the likelihood or impact of the risk to a resource. Continuity options are determined and planned for before a disruption to help ensure continuation of an essential business function during and after the disruption. An example of risk mitigation is purchasing a generator to decrease the risk of losing electricity needed to process vaccine orders. An example of a continuity option is preparing to use paper forms or an alternative online system (e.g., an online survey) to collect vaccine orders.

Risk mitigation strategies and business continuity options answer the question, "how will we avoid (risk mitigation) or respond (business continuity) to disruptions."

Risk mitigation strategies and business continuity options answer the question, "how will we avoid (risk mitigation) or respond (business continuity) to disruptions."

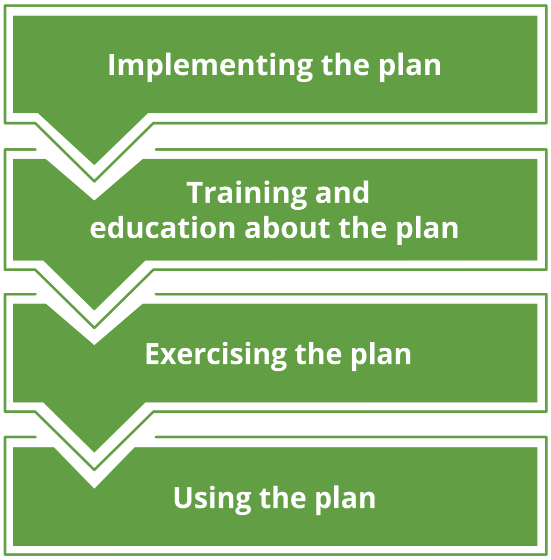
[17] Adapted from BCM Institute. Risk Mitigation. (2017, August 23). Retrieved April 1, 2019, from http://www.bcmpedia.org/wiki/Risk_Mitigation

Figure 1 | *Simple diagram of components in developing a business continuity plan*


BUSINESS IMPACT ANALYSIS
SELECTED ESSENTIAL BUSINESS FUNCTIONS
RISK ASSESSMENT
RISK
Answers "What?" and "When?"
Answers "Why?"
RISK MITIGATION STRATEGIES
Answers "How?" Done before a disruption
BUSINESS CONTINUITY OPTIONS
Answers "How?" Planned before a disruption, implemented after a disruption

2.5 POST-PLANNING ACTIVITIES: CONCEPTS TO SUSTAIN AND USE A BUSINESS CONTINUITY PLAN

- **Implementing the plan:** Successful use of a business continuity plan during a disruption requires more than just a written plan. Once the plan has been developed, ongoing work is needed to put risk mitigation strategies in place and develop tools and resources to support business continuity options.
- **Training and education about the plan:** Staff will need to be knowledgeable about the plan in order to use it during a disruption. Develop regular training and education opportunities to ensure that staff can use the plan when needed.
- **Exercising the plan:** Exercising a plan is done to "train for, assess, practice, and improve performance and capabilities in a controlled environment."[18] There are several methods for exercising a business continuity plan. The main goals of exercising are to practice the response to a disruption and to determine if the plan needs any updates or changes.
- **Using the plan:** If there is a disruption to a resource necessary for a business function, staff should be knowledgeable about the plan and prepared to respond to the disruption. The plan should be available through off-site storage in the event the primary location is inaccessible.



Each of these concepts is described in greater detail in Chapter 5 and Chapter 6.

[18] ISO 22313:2012(E), Societal security — *Business continuity management systems — Guidance*

2.5 SUMMARY

There is great value in creating a business continuity plan for an IIS program. Both the process of developing a plan and the utility of having predetermined the response to a disruption increase the likelihood that an IIS program will successfully resume normal operations after a disruption. A successful business continuity plan cannot exist in a void. To accomplish business continuity, an IIS program also needs to implement a business continuity management system that will support the ongoing use and improvement of a business continuity plan.

> “A good plan today is better than a perfect plan tomorrow.”
>
> — George S. Patton

3

BUSINESS CONTINUITY PLAN DEVELOPMENT PROCESS

3 BUSINESS CONTINUITY PLAN DEVELOPMENT PROCESS

This chapter describes the process of developing a business continuity plan. During the process of developing a business continuity plan, there are a few broad principles to keep in mind.

The principles in this guide are notated as PR-### and are further described in Chapter 7: Principles. A business continuity plan should:

- Address the following topics with respect to disruptions: prevention, risk mitigation, continuity of operations, response to a disruption, and resumption of normal operations (PR-001)
- Maintain applicable security and confidentiality requirements (PR-002)
- Ensure the integrity of all data maintained by an IIS that is impacted by a disruption (PR-003)

There are six tasks in the development process, and each task includes one or more steps. The process proceeds from Task 1 through 6. However, if there are changes to the program's business functions or risks after the plan is developed, consider repeating Tasks 3 through 6 to update the plan. The tasks and steps are described in detail in this chapter. Every task will benefit from engaging an appropriate group of subject matter experts (mainly IIS and immunization program staff) in discussions and planning. By taking the time to work with a group of subject matter experts, the plan will better reflect the reality of the IIS and IIS program, and there will be greater buy-in for the final business continuity plan.

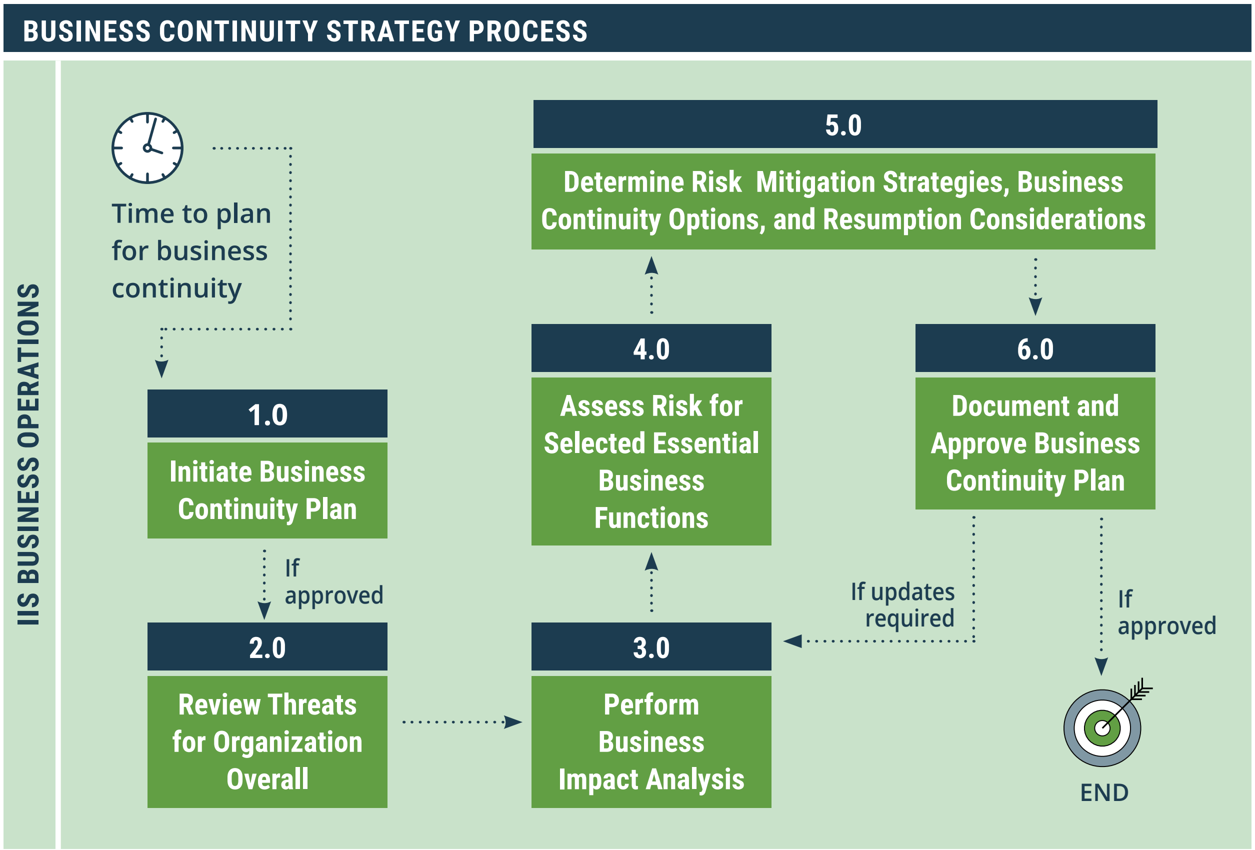
Development of a business continuity plan should follow the steps in this process to ensure that important elements of a plan are completed (PR-004). While following the steps of the process is recommended, there is significant flexibility in how a program implements several of the steps. IIS program staff are encouraged to implement the process in a manner that works well for their specific program.

Note: If the IIS business continuity plan is being developed as a part of a larger organization-wide initiative, there may be specific forms provided for the plan. It is still recommended that each IIS program perform the steps outlined below to ensure the creation of a plan that will be useful and sustainable for the IIS program.

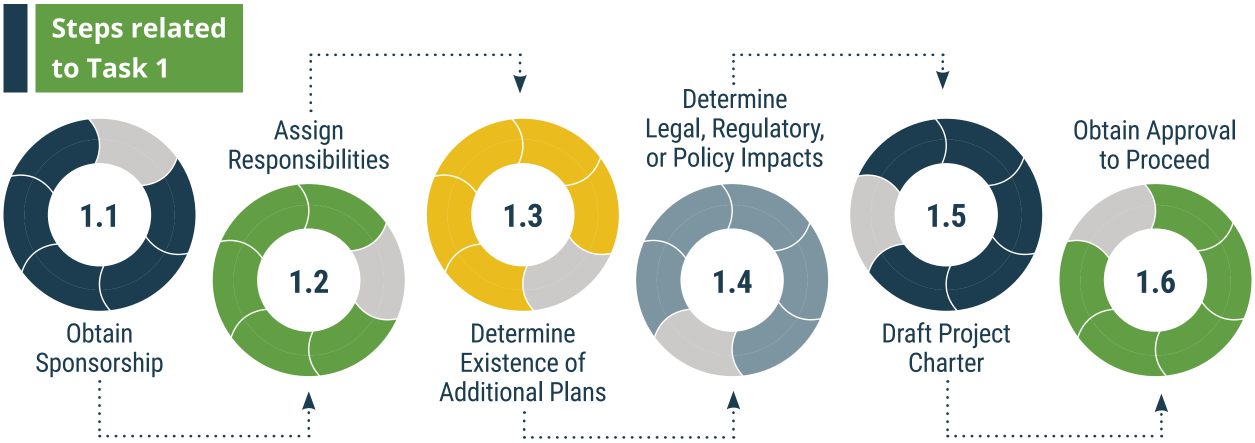
Creating a business continuity plan is an important step in ensuring ongoing business continuity for the IIS program and should be done concurrently with developing a business continuity management system. For example, once there is approval from leadership for developing a business continuity plan, get approval for the ongoing activities needed for a business continuity management system (e.g., training for the plan, as well as exercising, updating, and improving the plan). More information about the activities involved in a business continuity management system are in Chapter 5.

The following diagram shows the high-level tasks associated with the development of a business continuity plan. Each of these tasks consists of one or more steps detailed in this section. See Appendix U for a summary of the inputs and outputs for each task.

Figure 2 | *Tasks in the business continuity process*


BUSINESS CONTINUITY STRATEGY PROCESS
IIS BUSINESS OPERATIONS
Time to plan for business continuity
1.0
Initiate Business Continuity Plan
If approved
2.0
Review Threats for Organization Overall
3.0
Perform Business Impact Analysis
4.0
Assess Risk for Selected Essential Business Functions
5.0
Determine Risk Mitigation Strategies, Business Continuity Options, and Resumption Considerations
6.0
Document and Approve Business Continuity Plan
If updates required
If approved
END

TASK 1:
INITIATE BUSINESS CONTINUITY PLAN


Steps related to Task 1
1.1
Obtain Sponsorship
Assign Responsibilities
1.2
1.3
Determine Existence of Additional Plans
Determine Legal, Regulatory, or Policy Impacts
1.4
1.5
Draft Project Charter
Obtain Approval to Proceed
1.6

INPUTS

- Other business continuity plans that exist within the health department
- Legal, regulatory, or policy documents that impact the IIS
- Vision, mission, and goals of the IIS program
- Specific forms provided for the plan, if any

DESCRIPTION

The purpose of this task is to create a strategy for developing the business continuity plan and ensure that there are resources to support the development and sustainability of the plan. It is important to ensure there is buy-in for the activity from leadership and management. The individuals who are considered to be in leadership for the purpose of a business continuity plan will vary based on the structure of the organization and the source of funding for the plan. Leadership should demonstrate commitment to the business continuity plan (PR-005). By obtaining commitment from leadership, the business continuity plan and management system are more likely to be developed, given access to resources, and supported over time. Ensuring ongoing access to resources is particularly important. Sufficient resources should be made available to develop, adopt, exercise, put into place, and regularly review and update the business continuity plan (PR-006).

Early in the process, make important internal partners (e.g., emergency preparedness, central IT) aware of the plan for developing a business continuity plan and get insights from other areas of the organization (PR-007). Depending on the norms and expectations within an organization, this may occur early in this process or after gaining approval from leadership to proceed with the business continuity plan (Step 1.6).

STEP 1.1: OBTAIN SPONSORSHIP

In the first step of the process, select a project sponsor. The project sponsor will support and advocate for the project and assist with difficult decisions.[19] Project sponsors should be in a leadership role so that they can advocate for the project and help manage issues. Examples of possible project sponsors are the IIS manager, program manager, or a supervisor in the IIS program.

This step is a good time to start promoting the idea of a business continuity plan to leadership who can approve of the development of such a plan. This is also the appropriate time to begin identifying the resources needed to support the business continuity planning process. It is especially helpful to gather information about the availability of staff time for development of a plan.

In addition, this is a good time to determine who in leadership will need to approve the plan and what the approval process will require. The individuals who need to approve the development of the plan may be determined by:

- The health department's structure and policies
- The funding that will be used to develop the plan
- Whether the IIS business continuity plan is a part of a higher-level business continuity plan (e.g., division or agency)

Language from Chapter 2 can be used to explain the value of an IIS business continuity plan to leadership.

[19] A more detailed description of the role of a project sponsor is available at https://www.pmi.org/learning/library/importance-of-project-sponsorship-9946.

STEP 1.2: ASSIGN RESPONSIBILITIES

In this step, assign roles and responsibilities to the project team that will develop the business continuity plan if the project is approved (Step 1.6). If the project manager role is assigned first, that person can help identify other members of the team. The project manager will be responsible for organizing and coordinating the project.[20] The project manager will lead the development of a project charter and, with the project sponsor, communicate with leadership about the project. The following list provides a high-level description of the roles and responsibilities associated with developing a business continuity plan. While it is generally a good idea to have only one person acting as the project manager, multiple people can fill other roles.

PROJECT MANAGER

- Develops the project plan
- Coordinates the project team
- Manages relationships with project stakeholders and team
- Oversees communication
- Coordinates the project schedule and budget
- Mediates any project conflicts

WRITER

- Reviews additional plans and risk assessments that have previously been developed by the organization for input into the business continuity plan (Step 1.3)
- Documents the processes used in developing the plan
- Writes the business continuity plan
- Drafts internal and external communications

SUBJECT MATTER EXPERT REPRESENTATIVES FROM EACH AREA SUPPORTED BY THE IIS PROGRAM

- Participate in information-gathering sessions
- Consult with peers as needed
- Review and provide feedback on documentation and the drafted business continuity plan

OPTIONAL PARTICIPANTS (depending on the composition of the IIS program and the scope of the business continuity plan)

[20] A wealth of information about project management is available via the Project Management Institute (https://www.pmi.org/) and through the Public Health Informatics Institute's course Designing and Managing Public Health Information Systems: 8 Steps to Success (https://www.informaticsacademy.org/LearnerConnection/Menu4ia.aspx?&Host_Site=01&StartPage=CrseDesc&Continue=&PartNo=0005_ENU_20170321).

1.3

Determine existence of additional plans

STEP 1.3: DETERMINE EXISTENCE OF ADDITIONAL PLANS

Many health departments have high-level business continuity plans. In this step, determine if there are other business continuity plans for the health department. Identify any risk assessments and business impact analyses that have been done at a higher level in the health department. Also, check for business continuity plans/tools for similar programs within the health department (e.g., the disease reporting system, the cancer registry) that may help with the business continuity planning process. The business continuity plan should inform, comply with, and not contradict other applicable plans in the jurisdiction (PR-008). If discrepancies with other plans are discovered during the process of developing the IIS business continuity plan, either adjust the IIS business continuity plan or work with the owners of the other plan to fix the discrepancy. For more information about additional plans, see IIS business continuity plan vs. other plans in Chapter 2 and Integration into other state and agency plans in Chapter 4.

1.4

Determine legal, regulatory, or policy impacts

STEP 1.4: DETERMINE LEGAL, REGULATORY, OR POLICY IMPACTS

During this step, identify laws, regulations, or policies that may influence the IIS business continuity plan. The business continuity plan should inform, comply with, and not contradict applicable legislation, policies, and regulatory requirements (PR-009). There are different avenues to explore, including:

- Laws and regulations for privacy and security, such as the Health Insurance Portability and Accountability Act (HIPAA)[21]
- State laws dealing with emergency powers
- State laws dealing with IIS authorization
- State laws dealing with privacy and confidentiality

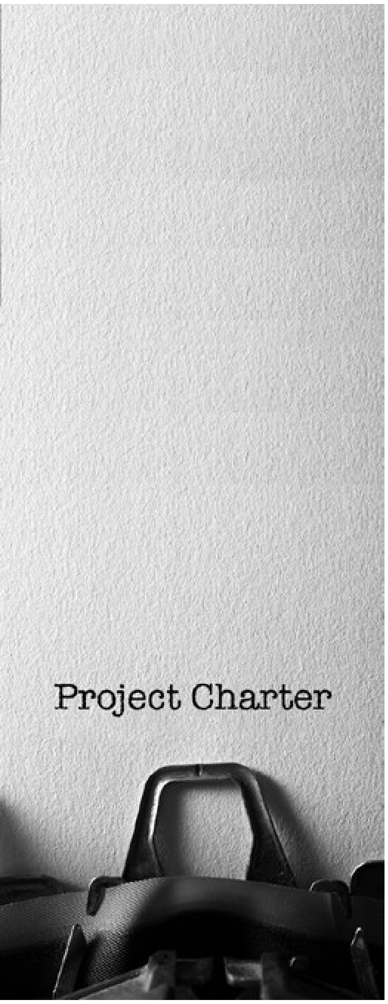
Staff with a legal or privacy officer background at the health department may need to assist with this task, which could make it a challenge to do in a timely manner. If it is not possible to accomplish this step within a reasonable amount of time, continue the review with the appropriate health department staff while moving forward with the next step in the process. Review the business continuity plan against applicable laws, regulations, or policies when writing and documenting the plan. (Step 6.1).

[21] For more information about laws and regulations for privacy and security, please see AIRA Confidentiality and Privacy: Considerations for IIS (https://repository.immregistries.org/resource/aira-confidentiality-and-privacy-considerations-for-iis/), AIRA Security Guidance Considerations for Immunization Information Systems (https://repository.immregistries.org/resource/security-guidance-considerations-for-immunization-information-systems/), and the HIPAA website (https://www.hhs.gov/hipaa/index.html).

STEP 1.5: DRAFT PROJECT CHARTER

At this step, draft a project charter. Use the vision, mission, and goals of the IIS program to help shape the project charter and scope of the activity. The project charter should include:

- A statement regarding what a business continuity plan is and why it is needed (language from Chapter 2 can be used for this portion of the charter)
- The scope of the activity for the business continuity planning process
    - The scope of the IIS business continuity plan will help determine what is addressed in the plan. Questions to consider in determining the scope of the plan include:
        - Will it address technical issues (e.g., issues with servers)?
        - Will it address issues related to an IIS vendor?
        - Will it include staff that is external to the IIS program or immunization program (e.g., regional IIS staff)?
    - Tailor the scope of this business continuity plan so that it does not duplicate items covered by existing continuity plans within the health department.
        - For example, if a high-level plan describes business continuity for disruptions impacting the facility that houses the IIS program, that topic might not need to be addressed in the IIS business continuity plan. Information obtained in Step 1.3 can help determine what is considered in-scope for the IIS business continuity plan.
- Objectives of the plan and assumptions for developing the plan
- A project timeline and high-level activities that are part of the business continuity planning process (a checklist of milestones is available in Appendix F)
- Documentation of the roles and responsibilities of those involved with the business continuity planning process
- Notes about the existing information that will be leveraged for creating the plan (information obtained in Step 1.3 and Step 1.4 may be included in these notes, if applicable)



STEP 1.6: OBTAIN APPROVAL TO PROCEED

In the final step of this task, request and obtain approval to proceed with the development of the IIS business continuity plan. The process for obtaining approval depends on the structure and standards of the health department; it may be casual or may involve a formal process or presentation. Activities in Step 1.1 should have identified which members of leadership need to approve the development of the plan. If approval is required from individuals who are not directly involved with the development of the business continuity plan, provide a clear explanation of why the business continuity plan is necessary for the operational integrity of the business functions supported by the IIS program.

Items that may be useful in assisting with obtaining approval:

- Project charter (Step 1.5)
- Budget and/or staff time needed for the development of the plan

Include an adequate amount of time in the project timeline for getting approval. If the approval process in the health department is a formal and/or lengthy process, the time to complete this step could have a significant impact on the overall project timeline.

Once approval has been received, staff and resources should be allocated, and the project sponsor and project manager can proceed with development of a business continuity plan and management system as described in the next tasks. Likewise, at this point, the project manager should ensure that important internal partners and leadership know an IIS business continuity plan is being developed (PR-007).

Approval for developing the business continuity plan should also include support for a broader business continuity management system. More information about the activities involved in a business continuity management system can be found in Chapter 5.

SUMMARY OUTPUTS

- Support from leadership
- Project roles and responsibilities
- Background materials about existing business continuity plans, business impact analyses, and risk assessments
- Background materials about legal, regulatory, and policy impacts on the business continuity plan
- Project charter
- Approval to proceed with development of a business continuity plan and management system
- Staff and resources allocated to proceed with development of a business continuity plan and management system

TASK 2:
REVIEW THREATS FOR ORGANIZATION OVERALL

Step related to Task 2

Perform a Threat Assessment

Threat assessment is the determination of the potential threats that may impact an organization and the likelihood of those threats occurring.

INPUTS

- Threat assessments that have been done in the health department

DESCRIPTION

The intent of this task is to create awareness of the potential threats to the IIS program and to review any threat assessments already completed for the health department.

Perform a Threat Assessment

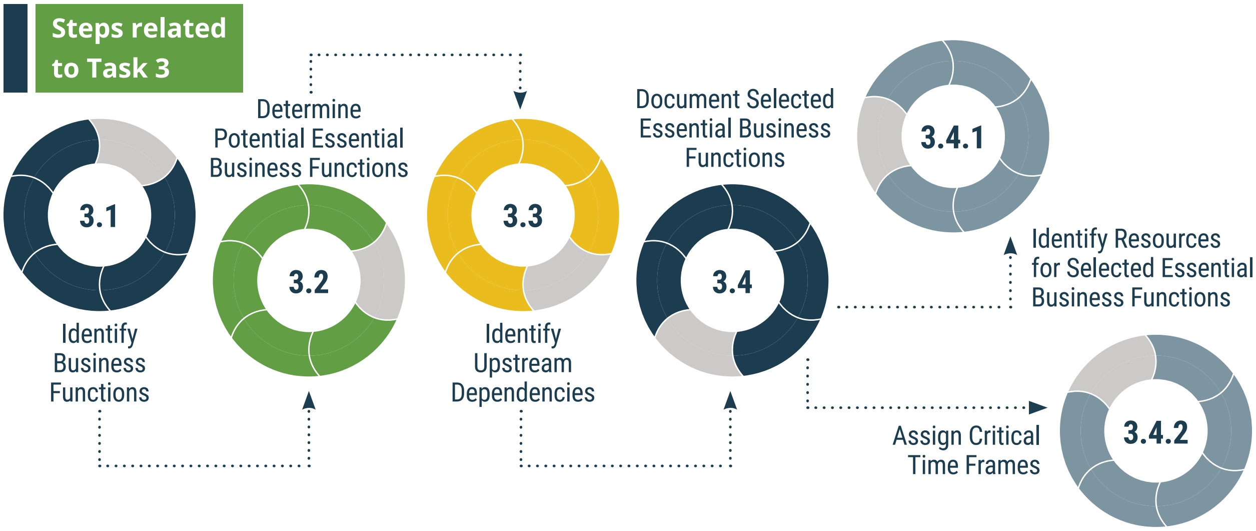
STEP 2.1:
PERFORM A THREAT ASSESSMENT

Threat assessment is the determination of the potential threats that may impact an organization and the likelihood of those threats occurring. Threats can be geological, meteorological, biological, or caused by humans (either accidentally or intentionally). While it is important to understand the types of threats and the impact they would have on the organization, it is not the intention of the business continuity plan for the IIS program to do a deep dive on this subject, as it has most likely already been done for the broader organization. Look at the scope of the threat assessments that have been done in the health department to determine if they cover important factors related to the IIS program (e.g., the facility housing the IIS staff).

SUMMARY OUTPUTS

- **Staff developing the business continuity plan has a general understanding of the threats that could impact the IIS program.**

TASK 3:
PERFORM BUSINESS IMPACT ANALYSIS


Steps related to Task 3
3.1
Identify Business Functions
3.2
Determine Potential Essential Business Functions
3.3
Identify Upstream Dependencies
3.4
Document Selected Essential Business Functions
3.4.1
Identify Resources for Selected Essential Business Functions
3.4.2
Assign Critical Time Frames

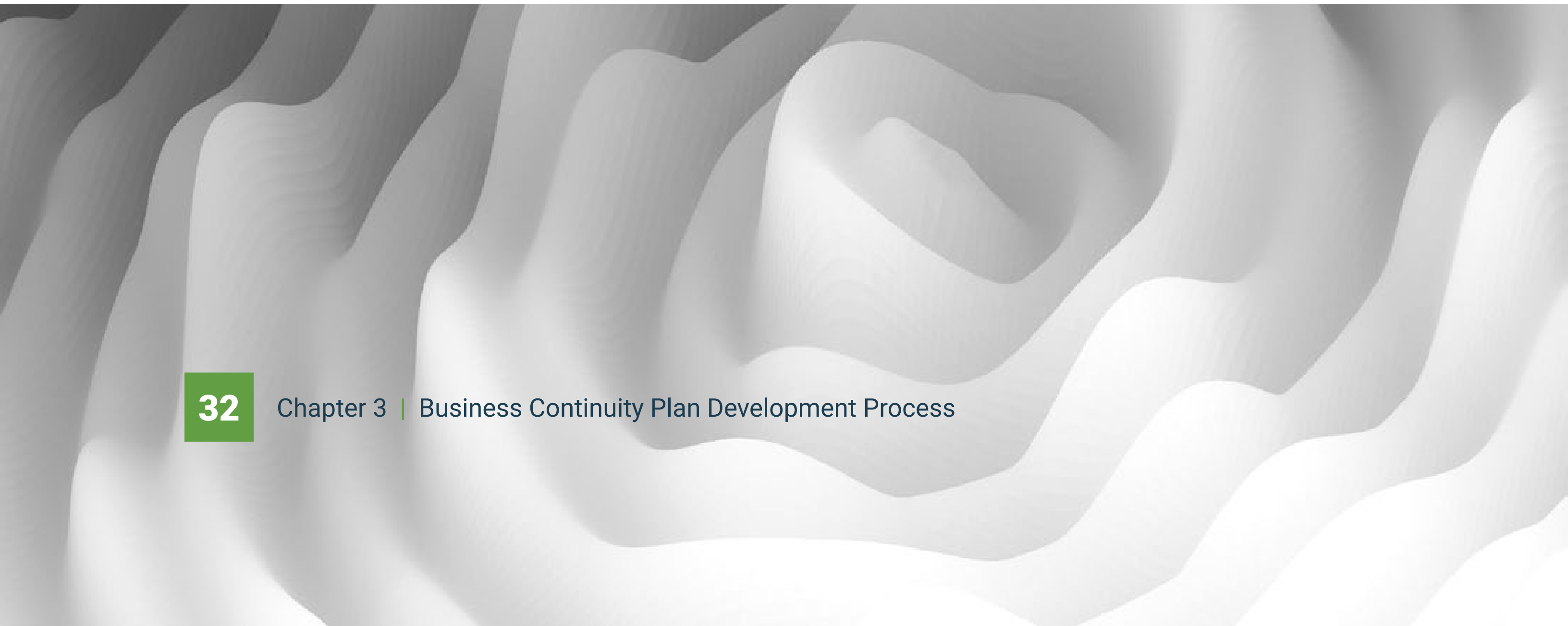
INPUTS

- Documents to support the identification of business functions that the IIS program supports (e.g., IIS strategic plan, IIS Functional Standards[22])

DESCRIPTION

Task 3 provides a step-by-step process for performing a business impact analysis to identify essential business functions and time frames related to resumption of the function. A description of business impact analysis is provided in Planning Activities: Concepts for developing a business continuity plan in Chapter 2.

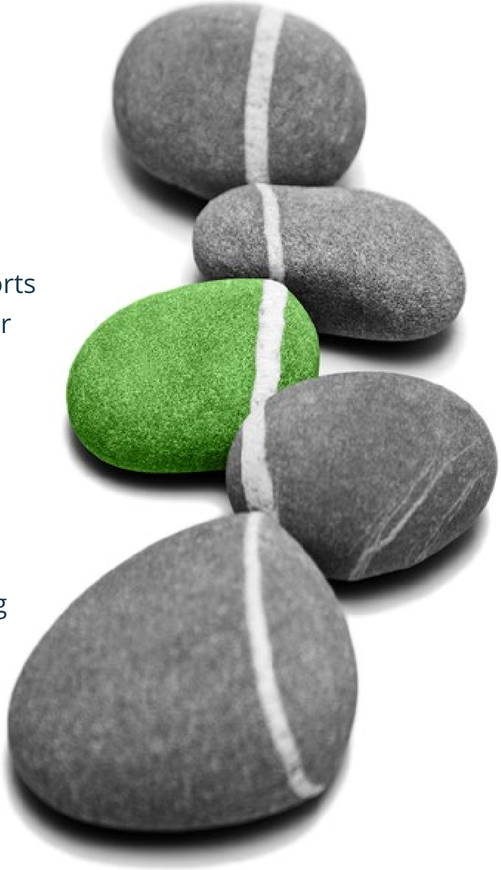
[22] https://www.cdc.gov/vaccines/programs/iis/func-stds.html



STEP 3.1: IDENTIFY BUSINESS FUNCTIONS

The first step in Task 3 is to identify business functions that the IIS program supports. This may involve reviewing several different sources. Suggested methods include the following:

- Review the legal obligations of the IIS to identify required business functions (e.g., mandate for providers to report to the IIS, mandate for IIS access by certain persons/entities).
- Review the IIS Functional Standards.[23]
- Review the list of applications and programs that the IIS program supports (e.g., Vaccines for Children [VFC], Immunization Quality Improvement for Providers [IQIP]).
- Review job descriptions for individuals with key roles in the IIS program to identify tasks and activities.
- Review the IIS strategic plan.
- Brainstorm with IIS staff and/or an oversight/advisory group (if one exists).
- Check additional resources to help identify business functions, including the CDC Immunization Program Operations Manual[24] and the Immunization and Vaccines for Children Cooperative Agreement.[25]



In this step, identify all business functions supported by the IIS program; then, as the business impact analysis progresses, the list of business functions will be reduced to a smaller number of selected essential business functions for inclusion in the business continuity plan

This is a significant step in the process, and it will require a substantial amount of time to complete.

[23] https://www.cdc.gov/vaccines/programs/iis/func-stds.html
[24] Available at the ISD Awardees SharePoint portal: https://cdcpartners.sharepoint.com/sites/NCIRD/PAP/SitePages/Home.aspx
[25] Ibid.

Determine potential essential business functions

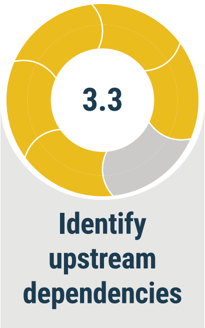
STEP 3.2: DETERMINE POTENTIAL ESSENTIAL BUSINESS FUNCTIONS

Using the list of business functions that was developed in Step 3.1, this next step provides a process to identify the business functions that are essential to the IIS program. The five factors that are listed below can be used to determine which business functions are considered potential essential business functions. IIS programs can determine if other factors should be considered in this process. Likewise, IIS programs can determine if factors should have equal weight or differing weights based on their importance. The IIS program should develop a table to record a "score" for each factor for each business function. An example of a table is included in Appendix G.

Factors to determine a potential essential business function

- **Time critical:** Is the business function time critical?
  - If the business function is not quickly resumed, are there significant repercussions?
  - Note: Time critical is a general concept in this question. A more detailed process for determining time frames for selected essential business functions occurs in Step 3.4.2.
- **Legal requirement:** Is there a legal requirement that the business function must be provided?
  - May be state mandated, or there may be other policy/legal requirements for a business function
- **Public health value:** Is there a high public health value to the business function?
  - Is there a potential public health threat if this business function is not performed?
- **Negative impact on customer:** Would the customers of the business function be negatively impacted if the business function was not available?
  - Is it a business function that is provided only by an IIS?
- **Reputation of IIS program:** Is there a potential impact to the reputation of the IIS program?
  - Would the stakeholders' faith in the benefit of the IIS program be harmed if the disruption lasts?
  - Note: The reputation of the IIS program, immunization program, and IIS partners should be considered when developing a business continuity plan.

Using the scores created for each business function, prioritize the top-scoring business functions to develop a list of potential essential business functions. It is not necessary for all five factors to apply to be considered a potential essential business function. For example, a business function could have high scores for four factors and a zero for the fifth factor and still be considered a potential essential business function.

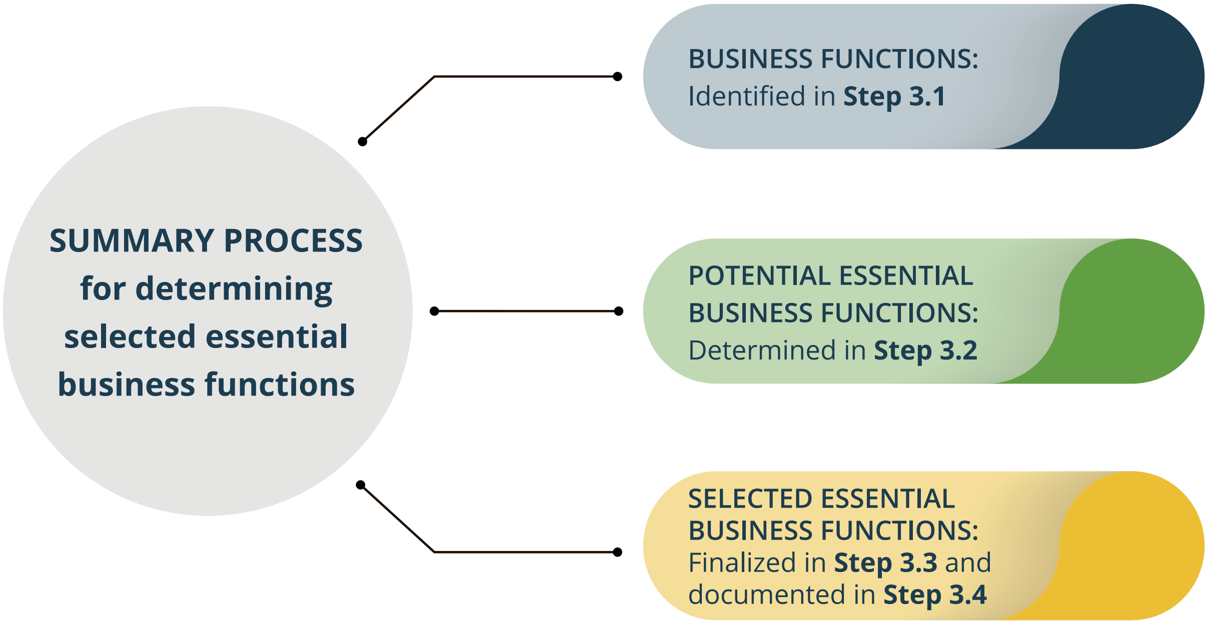


STEP 3.3: IDENTIFY UPSTREAM DEPENDENCIES

Once the potential essential business functions have been identified, determine the upstream dependencies associated with them. Upstream dependencies are the activities/processes that must occur for the potential essential business function to operate. The process of identifying upstream dependencies may highlight additional potential essential business functions that were not previously identified. For example, if a business function is an upstream dependency for several potential essential business functions, it may also be a potential essential business function. An example of this step is given in Appendix I.

At the end of this step, finalize a list of potential essential business functions that the IIS program has the time and resources to address in a business continuity plan. These business functions will be referred to as "selected essential business functions."

SCOPE CHECK: This is a good time to revisit the scope that was developed in Step 1.5 to make sure that the selected essential business functions are within the scope.



SUMMARY PROCESS for determining selected essential business functions

BUSINESS FUNCTIONS: Identified in **Step 3.1**

POTENTIAL ESSENTIAL BUSINESS FUNCTIONS: Determined in **Step 3.2**

SELECTED ESSENTIAL BUSINESS FUNCTIONS: Finalized in **Step 3.3** and documented in **Step 3.4**

The Business Continuity Workgroup identified a set of selected essential business functions (Appendix H). Each IIS program should combine use of the process recommended for this task together with the list of selected essential business functions developed by the Business Continuity Workgroup.

Document selected essential business functions

STEP 3.4: DOCUMENT SELECTED ESSENTIAL BUSINESS FUNCTIONS

For each selected essential business function, create a use case to document the normal operations (also referred to as "sunny day" use cases). Examples of use cases are available in Appendix J. Information from the use cases will be used in the following two sub-steps to determine the resources needed for the selected essential business function and the critical time frames.

Step 3.4.1: Identify Resources for Selected Essential Business Functions

For each selected essential business function, identify the resources needed to support the function's normal operations. The use cases that were developed in Step 3.4 can help identify the resources needed for the selected essential business function (see Appendix K). Once the resources have been identified, incorporate them into a table to allow for quick reference and comparison of resources (see Appendix L). The broad resource categories to consider are:

People who Support the Business Function // Example: IIS Program Staff

Information and Data // *Example:* Patient Demographic Information

Technology // *Example:* IIS

Buildings and Worksites // *Example:* IIS Program Facility

Communication Systems // *Example:* Internet

Equipment // *Example:* Computers

Utilities // *Example:* Electricity

Step 3.4.2: Assign critical time frames

For each selected essential business function, identify the critical time frames associated with the function. These critical time frames will be helpful in determining the type of risk mitigation and business continuity options that will be most applicable for the function. All three time frames are defined in Planning activities: concepts for developing a business continuity plan in Chapter 2.

During the process of determining critical time frames, it is important to balance the urge to quickly resume the business function with the availability of resources. While in an ideal world, all problems would be resolved immediately, costs can be unsustainably high when tight time frames are set.

For all selected essential business functions that involve electronic collection or storage of information, identify a recovery point objective (RPO) (PR-010). The RPO is the point prior to a disruption to which information used by a business function must be restored in order to minimize the loss of data resulting from the disruption. This time frame helps determine what frequency of backups is needed and provides insight about how much data could be lost due to a disruption.

A recovery time objective (RTO) should be determined for all selected essential business functions (PR-010). The RTO is the period of time following a disruption within which a business function must be resumed. The business function can be resumed by an alternate process or by restoring normal operations. The RTO can be a specific amount of time (e.g., 48 hours) or priority levels associated with ranges of time. An example of levels[26] would be:

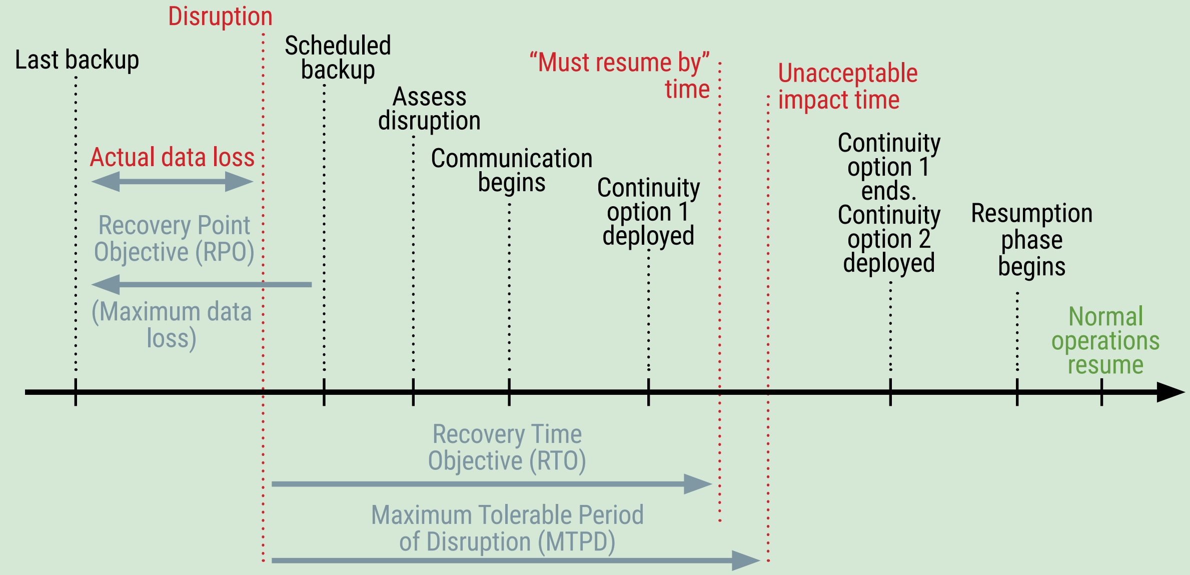
LEVEL	RESUMPTION OF BUSINESS FUNCTIONS MUST OCCUR WITHIN
1	0 – 12 hours
2	12 – 48 hours
3	2 – 7 days
4	1 week – 2 months

[26] Roughly based on the Colorado Department of Public Health and Environment's COOP Annex

A third critical time frame that may be considered useful for certain IIS programs or selected essential business functions is maximum tolerable period of disruption (MTPD). MTPD is the time it would take for adverse impacts that might arise as a result of not providing a business function to become unacceptable. Like RTO, resumption of the business function can be by achieved an alternate process or through restoring normal operations. Unlike RTO, there is not an expectation that MTPD should be done for every selected essential business function. MTPD may be used if it is determined to be helpful in determining timelines for business continuity planning or for developing contracts with vendors/centralized IT.

Figure 3 | *Illustration showing how the time frames are related*

TYPICAL BUSINESS CONTINUITY SCENARIO



Notes for RPO:

- Disruption can happen at any time between backups.
- Actual data loss should always be less or equal to maximum data loss (RPO).
- Time between backups should always be less or equal to maximum data loss (RPO).

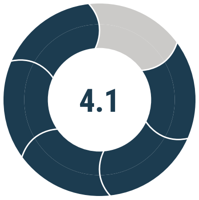
An option for comparing the critical time frames of multiple selected essential business functions is to develop a critical time frame table (see Appendix M). This table can be helpful in providing a quick visual reference for IIS staff and leadership about the time frames involved with business continuity for the IIS program.

SUMMARY OUTPUTS

- A list of business functions related to the IIS program
- A list of selected essential business functions
- Use cases for selected essential business functions
- A table of resources needed for selected essential business functions
- Critical time frames for selected essential business functions

TASK 4:
ASSESS RISKS FOR SELECTED ESSENTIAL BUSINESS FUNCTIONS

Step related to Task 4



Perform a Threat Assessment

INPUTS

- A table of resources needed for selected essential business functions (developed in Step 3.4.1)

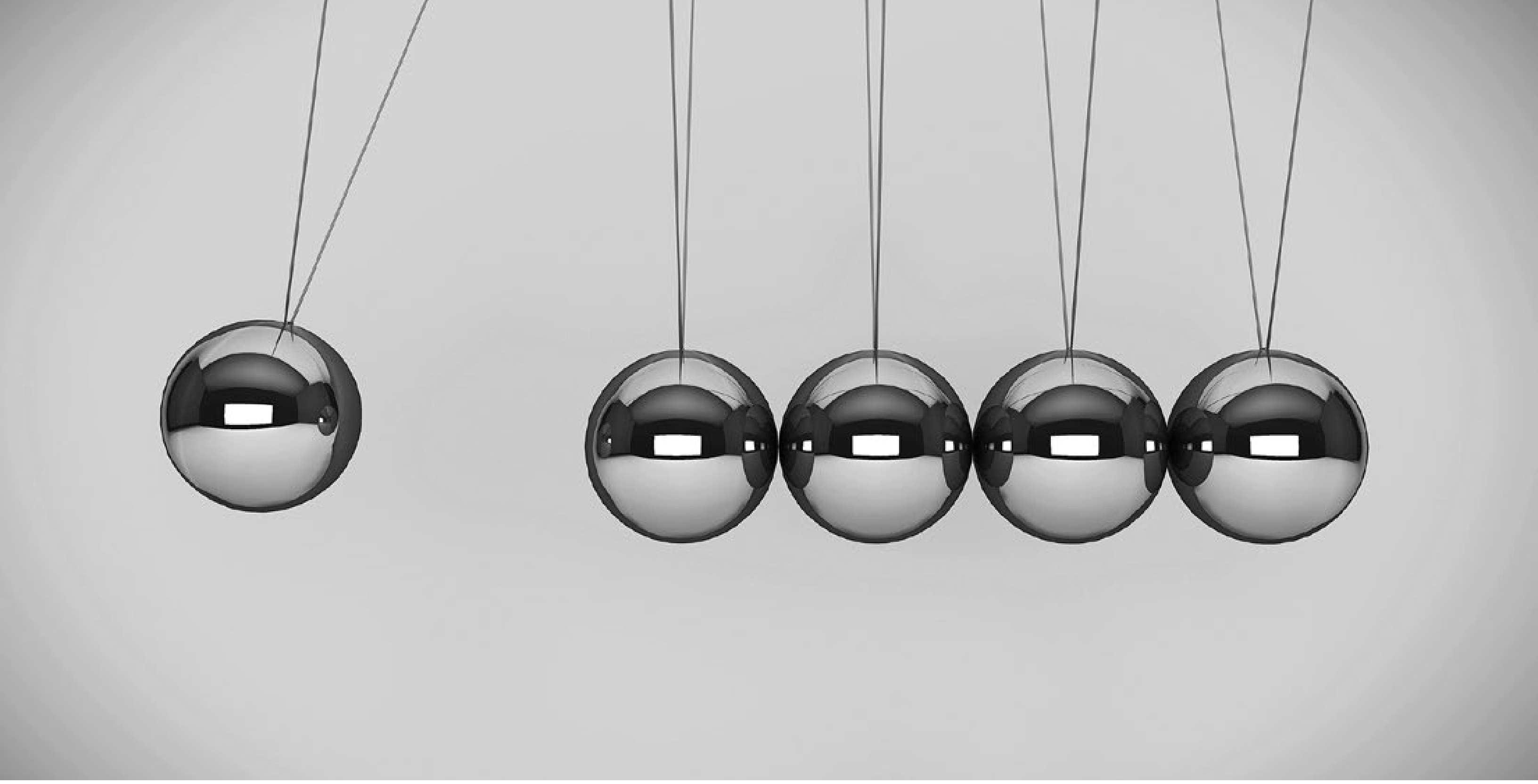
DESCRIPTION

Determine the calculated risk for each resource identified for each selected essential business function (developed in Step 3.4.1). This process will help determine which resources should be targeted for risk mitigation strategies and business continuity options.

STEP 4.1: PERFORM A RISK ASSESSMENT

Calculate the risk for each resource used by a selected essential business function. Risk should be analyzed in terms of consequences (impact) and likelihood (probability) (PR-011). This activity is best accomplished by bringing together a group of subject matter experts and discussing the probability and impact of each resource for each selected essential business function. A table that can be used for scoring resources by selected essential business function is available in Appendix N.

This table also includes space to document the responsible party (i.e., who is responsible for ensuring that the resource is available for the selected business function). Risk for all resources should be considered initially, even if the resource is not the responsibility of the IIS program or immunization program. Understanding that a resource plays a critical role in an essential business function supports communication with and education for the responsible party about the need for that resource. The IIS program may be able to make suggestions, even if it is not directly responsible for the resource.



It is useful to set and define the scales for probability and impact. A broader scale (e.g., 1–10) offers more room for nuance than a narrow scale (e.g., 1–3) but can also take more time to define and ensure that subject matter experts understand. It is also possible to have different size scales for probability and impact if one of the two factors should have a bigger effect on the calculation of risk. For example, if the subject matter experts feel that impact should have a higher effect on the calculated risk than probability, the scale for impact could be bigger than the scale for probability.

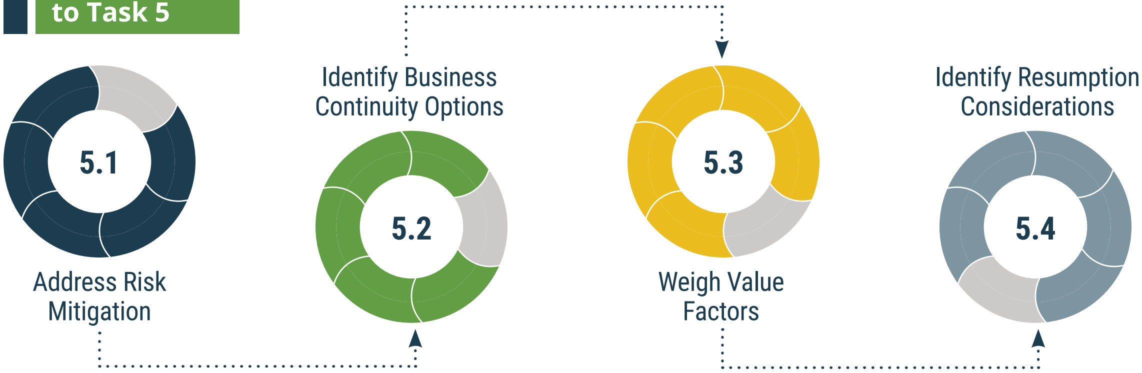
While the actual use of the calculated risk table may vary by IIS program, the process of working through the various steps ensures there is a good understanding of the risks to the resources needed by the selected essential business functions. Once the table is complete, identify a subset of the resources (by selected essential business function) that are considered most important to address via risk mitigation and/or business continuity options. This may be based on a variety of factors, including calculated risk and responsible party (e.g., it might be better to include a resource if the IIS program is the responsible party).

SUMMARY OUTPUTS

- A table with the calculated risks for resources needed for each selected essential business function
- A subset of resources (by selected essential business function) that are considered most important to address via risk mitigation and/or business continuity options

TASK 5: DETERMINE RISK MITIGATION STRATEGIES, BUSINESS CONTINUITY OPTIONS, AND RESUMPTION CONSIDERATIONS

Steps related to Task 5


5.1
Address Risk Mitigation
5.2
Identify Business Continuity Options
5.3
Weigh Value Factors
5.4
Identify Resumption Considerations

INPUTS

- Use cases for selected essential business functions (developed in Step 3.4)
- A table of resources needed for selected essential business functions (developed in Step 3.4.1)
- Critical time frames for selected essential business functions (developed in Step 3.4.2)
- A subset of resources (by selected essential business function) that are considered most important to address via risk mitigation and/or business continuity options (developed in Task 4)

DESCRIPTION

At this step in the process, the risks to resources and selected essential business functions are addressed with risk mitigation strategies and business continuity options.

Risk mitigation is done before a disruption to decrease the likelihood of a risk or impact of the risk on a resource. Continuity options are determined and planned for before a disruption to help ensure continuation of an essential business function during and after the disruption.

Risk mitigation strategies and business continuity options include:

- **Relocation:** The transfer of people or activities to another physical location, as determined by leadership/management
  - For example, moving IIS staff to a different building if there is a fire in the normal building
- **Alternative process (i.e., workaround):** A different way of doing something for a short period of time
  - For example, using paper forms or an online survey tool to collect orders if IIS vaccine ordering functionality is disrupted
- **Service delivery:** A method of delivering a service offered by a business function
  - For example, getting support from other agency help desk staff if there are several IIS help desk staff members out of the office because of illness

In certain situations, risk mitigation strategies or business continuity options may be cost- or resource-prohibitive. The IIS should still perform the other steps prescribed in a business continuity plan. For example, if vaccine evaluation and forecasting functionality is disrupted, it might not be cost-effective to perform a business continuity option; however, the IIS program should still communicate about the disruption, devote resources to resolve the issue, and educate users about how to proceed during the disruption. In situations where the planning process leads to the determination that risk mitigation strategies and business continuity options should not be developed or used, it is important to document the decision-making process that led to that determination.

STEP 5.1: ADDRESS RISK MITIGATION

In this step, use the subset of resources (by selected essential business function) that are considered most important to address from Task 4 and develop risk mitigation strategies that would either decrease the probability of the resource being disrupted or decrease the impact if the resource is disrupted. Examples of tables with risk mitigation strategies are included in Appendix O. Options for responding to risks include:

- **Mitigate or limit:** This option decreases the probability or impact of a risk occurring but does not completely remove the risk. An example of mitigating or limiting risk would be to cross-train additional staff to work on the IIS help desk. This would not remove the impact of not having enough staff to run the help desk, but it would reduce the probability of it.
- **Avoid:** This option fully removes the risk. This can occur by ceasing to use a resource or perform a selected essential business function (the latter would be highly unlikely). For example, an IIS program could determine that use of an old external database for a selected essential business function could be discontinued and, thereby, that specific risk could be avoided.
- **Share/transfer:** This option can be accomplished by moving the risk to a third party. This could involve contracting with a vendor to provide a service or resource. An example of sharing or transferring risk could be using servers or the cloud through a vendor rather than having an in-house server.
- **Accept:** This option allows an organization to accept that a risk exists without performing any actions to avoid or mitigate the risk. Even though this option does not reduce risk, it may be a good option for risks that are low probability and low impact. Likewise, it may be the most feasible option if the cost of risk mitigation strategies would be larger than the cost of the risk creating a disruption. An example of accepting a risk would be recognizing that it is possible that IIS staff could lose access to the internet but determining the probability and impact of the risk are low enough that the risk does not need to be avoided or mitigated. It is important to document the reasons for accepting a risk. A consideration when preparing the strategy of accepting a risk is the organization’s appetite for risk. Confirm with leadership that they are comfortable with the risks that will not be mitigated, avoided, or shared.

5.2

Identify business continuity options

STEP 5.2: IDENTIFY BUSINESS CONTINUITY OPTIONS

To identify business continuity options, consider measures that could help manage the disruption of a selected essential business function due to the loss of a resource. For example, what measures could be used to support vaccine ordering if the IIS vaccine ordering functionality stopped working? It is also important to consider the critical time frames that were developed in Step 3.4.2 to ensure that implementation of the business continuity options can meet these timelines.

There are several processes and tools that can guide the development of business continuity options:

- Work with a group of subject matter experts to develop a list of possible options. An example is available in Appendix P.
- Apply a business continuity option to the use case for the selected essential business function to help determine how the option could work. The initial use case was developed in Step 3.4, and an example of applying a business continuity option to a use case is provided in Appendix Q.
- Develop a timeline to help visualize the timing of activities to implement the continuity option. An example is available in Appendix R.

5.3

Weigh value factors

STEP 5.3: WEIGH VALUE FACTORS

Using the risk mitigation strategies and business continuity options that were developed in Step 5.1 and Step 5.2, this step determines which strategies and options are most reasonable to implement. Priority for development of risk mitigation and business continuity options should be placed on the most risk-prone resources and most impactful essential business functions. The process of narrowing the focus of planning to these resources and business functions largely occurred in the past two tasks; however, this step is a good opportunity to reassess the developed strategies and options to ensure that they meet this need.

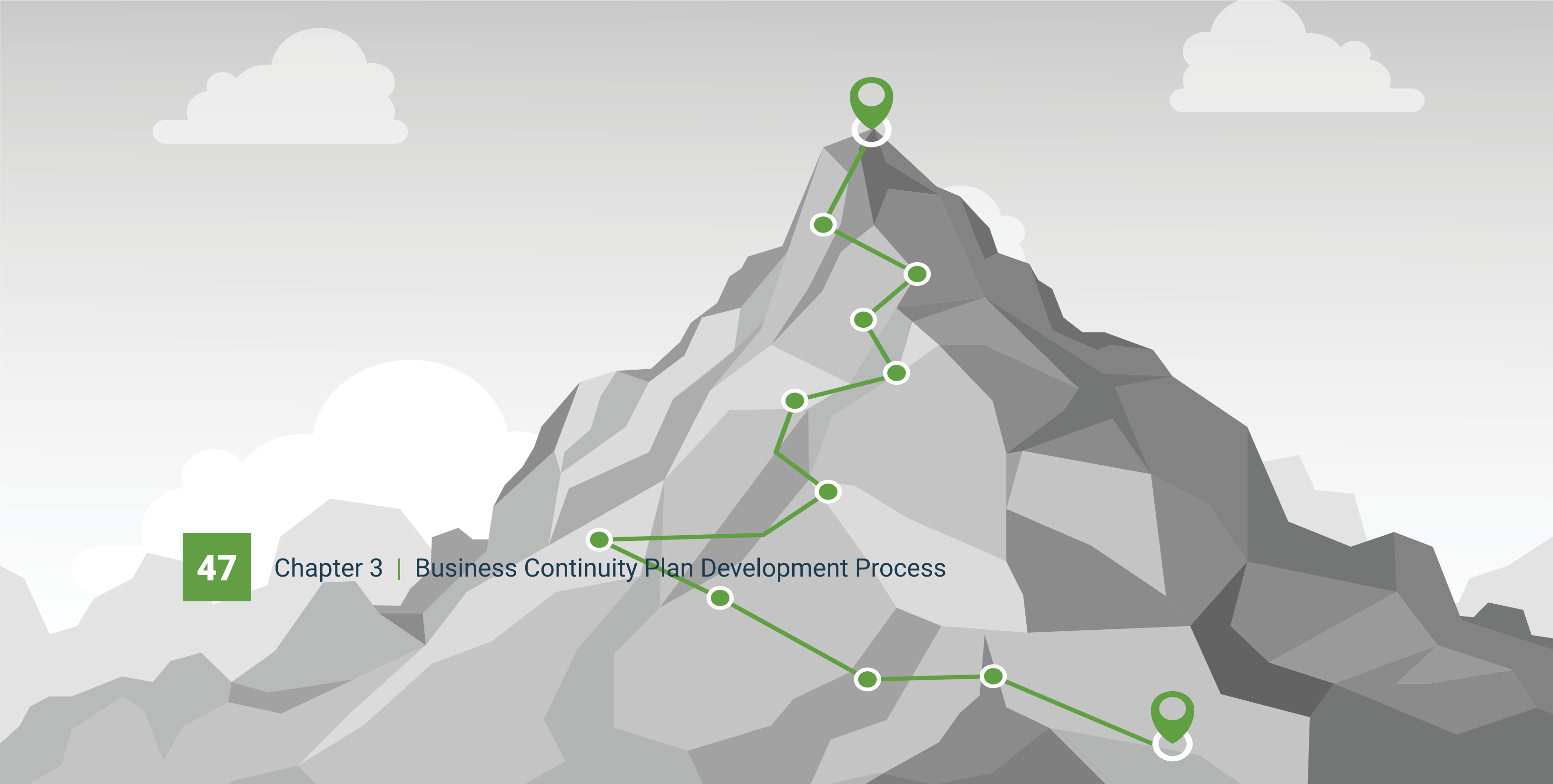
Priority for development of risk mitigation and business continuity options should be placed on the most risk-prone resources and most impactful essential business functions.

Priority should also be placed on cost-effective strategies and options. In order to do this, estimate the cost and effort associated with the risk mitigation strategies and business continuity options. For example, additional costs associated with communication would be minimal, whereas the cost associated with developing new IT functionality may be prohibitive.

Additional factors to consider in selecting which strategies and options to implement include:

- **Ease of implementation:** Activities that require IT development may be more complicated than nontechnical strategies.
- **Time required for implementation:** If the activity takes a significant amount of time, it may be difficult to implement and might not meet the RTO associated with the business need.
- **Groups responsible for implementation:** Depending on what individuals or groups bear the burden of the strategies and options, implementation may be easier or harder. For example, if all providers need to change their workflow for a business continuity option, it will likely be harder to implement than an option that just changes the workflow for IIS staff.
- **Interdependency:** If the activity requires another organization or group to work with the IIS program, it may make implementation more complex.
- **Legal obligation or policy:** If there is a legal obligation or policy requiring that a selected essential business function occur, there may be more support for strategies and options that ensure that the function is available.

Based on the factors listed above, determine which risk mitigation strategies and business continuity options should be included in the business continuity plan.



5.4

Identify resumption considerations

STEP 5.4: IDENTIFY RESUMPTION CONSIDERATIONS

In the final step in Task 5, use the selected essential business functions and high-risk resources to practice resumption planning. Resumption considerations assist with the process of restarting normal operations after a disruption has ended. It can be difficult to do significant pre-planning for resumption since it is often highly dependent on the specifics of the disruption (e.g., length of time, business continuity options performed). However, practicing the process of developing resumption considerations can help determine broad concepts or questions to consider when restarting normal operations.[27] Examples of questions that can be helpful during resumption are available in Appendix S.

Resumption considerations assist with the process of restarting normal operations after a disruption has ended.

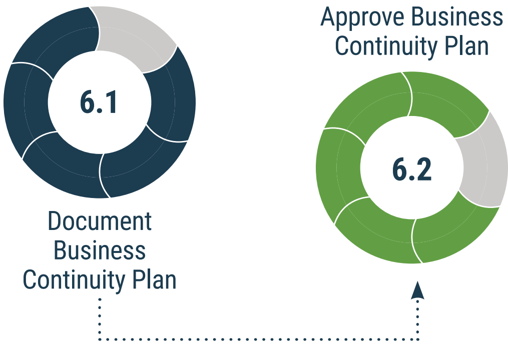
[27] For more about standing down after a disruption, see General standing down procedures in Chapter 6.

SUMMARY OUTPUTS

- Risk mitigation strategies for the subset of resources (by selected essential business function) that are considered most important to address
- Business continuity options for the selected essential business functions
- A subset of risk mitigation strategies and continuity options that the IIS program plans to implement and use
- A set of general concepts/questions that can be used to resume normal operations

TASK 6:
DOCUMENT AND APPROVE BUSINESS CONTINUITY PLAN

Steps related to Task 6



6.1
Document Business Continuity Plan
Approve Business Continuity Plan
6.2

INPUTS

- Project charter (developed in Step 1.5)
- Individual roles and responsibilities for implementing and maintaining the plan
- Contact lists (this could include lists of staff, vendors, suppliers, users, and other interested parties)
- A subset of risk mitigation strategies and continuity options that the IIS program plans to implement and use (developed in Step 5.3)
- A set of general concepts/questions that can be used to resume normal operations (developed in Step 5.4)

DESCRIPTION

The final task in this process is to document and get approval for the business continuity plan.

STEP 6.1: DOCUMENT BUSINESS CONTINUITY PLAN

In this step, develop general sections of the business continuity plan, incorporate business continuity planning that was completed in previous steps, and finalize the full business continuity plan.

Sections of a business continuity plan

SECTION	NOTES
Introduction	The purpose, scope, objectives, and assumptions used to develop the plan—update language from the draft project charter (Step 1.5).
Roles and Responsibilities	Individual roles and responsibilities for implementing and maintaining the plan.
Contact Lists	Depending on the needs of the IIS program, this could include lists of staff, vendors, suppliers, users, and other interested parties. Updates should be made as changes occur. The plan might not include the actual list of contacts but may point to how the list can be accessed (e.g., a database or organizational chart). This ensures that the most up-to-date contact list is available.
General Internal Communications	Guidelines on who would be contacted internally and when and how to contact them about disruptions (see Communication in Chapter 4 and Appendix T for more information).
General External Communications	Guidelines on whom to contact externally (e.g., users, partners, interested parties) and when and how to contact them about disruptions (see Communication in Chapter 4 and Appendix T for more information).
General Risk Mitigation Strategies and Continuity Options	Provide information about activities that apply to most or all risk mitigation strategies and/or continuity options (e.g., initial assessment of the disruption, recording of decisions and actions taken during a disruption).
Detailed Risk Mitigation Strategies for Each Selected Essential Business Function	A description of risk mitigation strategies that are planned for the selected essential business functions. These risk mitigation strategies were developed in Step 5.1, and a subset was selected in Step 5.3.
Detailed Continuity Options for Each Selected Essential Business Function	A reader-friendly procedure for business continuity options that can be performed during disruptions to the selected essential business functions. It is helpful to include information about roles and responsibilities related to the continuity options. These business continuity plans were developed in Step 5.2 and a subset was selected in Step 5.3.
General Resumption and Standing-Down Procedures	General information about resumption of the normal process for the business functions and standing down of any continuity options used in response to a disruption. Concepts from Step 5.4 can be used in this section. More information about standing down after a disruption is included in General standing down procedures in Chapter 6.

Once the business continuity plan has been drafted in its entirety, circulate the drafted plan for review and edits. The following people may be helpful reviewers of the plan: subject matter experts involved in creating the plan; individuals who will implement the plan in a disruption; and appropriate leadership (e.g., the IIS manager, immunization program manager). In addition, it may be beneficial to have someone in the immunization program who did not work on the plan review it to provide a fresh set of eyes. Additional partners (e.g., emergency preparedness staff, central IT staff, IIS vendor) may also provide helpful feedback at this step. Gather feedback from these reviewers and update the plan as needed.

6.2

Approve business continuity plans

STEP 6.2: APPROVE BUSINESS CONTINUITY PLAN

The final step in this process is to gain approval for the plan. As in Step 1.6, the process for obtaining final approval of the business continuity plan will depend on the structure and standards of the health department; it may be casual or may involve a formal process or presentation. This is also an important time to emphasize the critical nature of ongoing support for the broader business continuity management system.

Once the business continuity plan has been formally approved, make sure to communicate with internal and external partners:

- That the plan is approved
- How it can be accessed (for those that should have access)
- The plan for education about the plan and exercising the plan (see Chapter 5)

This is also an important time to emphasize the critical nature of ongoing support for the broader business continuity management system.

SUMMARY OUTPUTS

- A finalized and approved business continuity plan
- Communications to internal and external partners about the plan

4

BROAD CONCEPTS THAT APPLY TO THE BUSINESS CONTINUITY MANAGEMENT SYSTEM

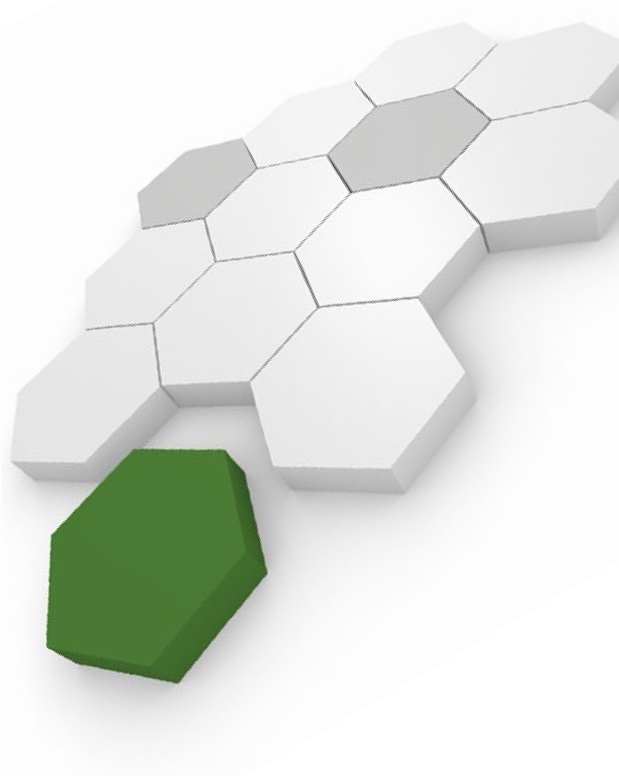
4 BROAD CONCEPTS THAT APPLY TO THE BUSINESS CONTINUITY MANAGEMENT SYSTEM

4.1 INTEGRATION WITH OTHER STATE AND AGENCY PLANS

> In some jurisdictions, continuity planning for functions of the IIS program may already be incorporated into existing organizational plans, including disaster recovery plans, COOP plans, incident management plans, or agency-level business continuity plans (a list of types of plans is available in Appendix E).

Prior to developing a business continuity plan, an IIS program should connect with its legal department, office of emergency preparedness, and/or executive office to gain insight on existing plans. This is outlined in Step 1.3 in Chapter 3. Enough time should be built into the development process to get the information requested from other areas of the organization prior to development of the IIS business continuity plan.

IIS programs may have limited input on these larger plans, but there may be an opportunity to provide feedback on the larger plan, incorporate the IIS business continuity plan into the existing plan, or include IIS-specific information in an appendix or annex to the larger agency plan. Incorporating IIS-specific components into these plans may be as simple as including a link to the IIS business continuity plan and may also be beneficial in securing additional funding for developing an IIS-specific business continuity plan and getting leadership buy-in.



Even if other existing state or agency plans mention the IIS, it is still important for the IIS program to develop its own business continuity plan. The IIS business continuity plan should inform and comply with other applicable plans in the jurisdiction and not contradict the content of those plans (PR-008). During disruptions that affect areas of the agency beyond the IIS program, these higher-level plans may take precedence over the IIS business continuity plan. Conversely, disruptions that affect only the IIS program will not trigger a higher-level plan and will be controlled by the IIS business continuity plan. To the extent possible, ownership and maintenance of the IIS business continuity plan should remain with the IIS program.

The IIS business continuity plan should inform and comply with other applicable plans in the jurisdiction and not contradict the content of those plans.

4.2 PROGRAM RESOURCES

Sufficient resources are necessary to develop, adopt, exercise, implement, and regularly review and update a business continuity plan (PR-006). Leadership support for embarking on this process helps ensure the availability of resources before getting further along in the development process. Leadership support is also important in making the plan a priority of the IIS program and immunization program when there are many competing priorities. In the process of developing the plan, finance and administrative procedures should be developed to support the activities in the business continuity plan before, during, and after a disruption (PR-012).

Sufficient resources are necessary to develop, adopt, exercise, implement, and regularly review and update a business continuity plan.

Dedicated staff time is needed to conduct the steps of the business continuity planning process and also to maintain the plan going forward. Business owners that have functions supported by the IIS program, such as the VFC program, are important stakeholders that should be at the table when developing the plan. Additional staff may include a project manager/owner, writers, subject matter expert representatives from each area supported by the IIS program, IIS vendor(s), IT staff, emergency preparedness staff, and communication staff. The amount of staff time allotted to this project may determine the scope of the plan and the number of selected essential business functions that will be addressed in the plan. Financially, the cost of staff time is likely the largest expense of developing a business continuity plan.

The process of developing a business continuity plan requires dedicated resources. But in addition to producing a useful plan, it also allows for critical thought on all the functions that the IIS program supports and where vulnerabilities exist. The time spent thinking through the process may prove to be beneficial for other purposes. For example, developing a business continuity plan can lead to better written procedures about business functions, which is helpful for standardizing processes and training new staff. This guide can help describe the benefits of having a business continuity plan as justification for dedicating resources toward the endeavor.

4.3 COMMUNICATION

COMMUNICATION-RELATED SECTIONS OF THE PLAN

In addition to communication during the development of the plan, as mentioned in Step 1.6 in Chapter 3, communication is crucial throughout a disruption. This guide recommends that the business continuity plan include sections on general internal communications and general external communications. The communications sections should outline which internal and external users should be included in communications once a disruption occurs. Utilizing multiple communication channels is important to ensure all appropriate audiences are reached, and consistent, uniform formatting of all communications easily identifies that the communication pertains to the disruption. The sections should also include general guidelines on what messages should be included and how to communicate those messages. Close-out communications to inform both internal and external partners that the disruption has been resolved are also an important final step in the process.

COMMUNICATION-RELATED SECTIONS OF THE PLAN: INTERNAL COMMUNICATIONS

An internal communication plan should include information on when to communicate with specific internal staff and when to escalate a situation to leadership.

An internal communication plan should include information on when to communicate with specific internal staff and when to escalate a situation to leadership. Methods of communication may include listservs (i.e., email), internal web pages, or phone trees. Depending on the extent of the disruption, routine updates may be necessary. It is also important that all staff is trained on consistent messaging to relay to external partners. Staff responsible for communicating messages externally should be designated. Depending on the extent of the disruption, this responsibility may fall outside of the IIS program and to agency leadership.

COMMUNICATION-RELATED SECTIONS OF THE PLAN: EXTERNAL COMMUNICATIONS

External communications include messaging to partners, IIS users, and other stakeholders. It is important that communications are tailored to the audience and convey the appropriate amount of information about the disruption and its impact. There may be routine communication methods, such as listservs, messages on social media pages, Health Alert Networks (HANs), or announcements on the IIS web page that can serve this purpose. Any changes in normal operations and action steps required on the part of the user should be clearly outlined. It is important that all communications are clear and concise and use plain language. It may also be helpful to incorporate best practices related to risk communications into the development of messages.[28] Approval for these external messages may be needed based on the type of external communication used and typical processes of the agency.

External communications include messaging to partners, IIS users, and other stakeholders. It is important that communications are tailored to the audience and convey the appropriate amount of information about the disruption and its impact.

Depending on the disruption, there may be a need for more robust staffing of an IIS help desk or other dedicated resources to help address questions or concerns. Using a standard voicemail greeting from the help desk acknowledging the disruption and what is being done to address it may help divert questions.

Another important part of external communication is ensuring appropriate contact lists are regularly maintained. This may include lists of VFC providers, health systems, and electronic health record (EHR) vendors. Consider how to best target other groups of users, such as working with a state agency to obtain a list of contacts at child care centers and schools for communication to those user groups. The contact lists should be kept outside of the IIS to ensure access to the lists during a disruption. Ensuring that specific groups of IIS users can be notified allows for targeted messages. This helps avoid overcommunication and messages being disregarded.

[28] For more information about risk communication, see https://www.cdc.gov/healthcommunication/risks/index.html.

5

POST-PLANNING ACTIVITIES OF THE BUSINESS CONTINUITY MANAGEMENT SYSTEM

Once the IIS business continuity plan has been documented, the risk mitigation strategies and business continuity options identified in the plan should be developed.

5 POST-PLANNING ACTIVITIES OF THE BUSINESS CONTINUITY MANAGEMENT SYSTEM

5.1 IMPLEMENTING THE PLAN

Once the IIS business continuity plan has been documented, the risk mitigation strategies and business continuity options identified in the plan should be developed.

Risk mitigation strategies may necessitate cross-training of staff, securing additional resources, or other preparation. Tools and resources to support business continuity options should be developed ahead of time so that, during a disruption, implementation can be done quickly. For example, if paper ordering forms or an online survey for vaccine ordering are part of a business continuity plan, they should be developed well before a disruption. Staff and resources will be necessary to support the implementation of the risk management strategies and business continuity options.

5.2 TRAINING AND EDUCATION

Developing and implementing a competency-based training and education curriculum that supports all individuals who have a role in the business continuity plan is vital for integrating the business continuity plan into practice (PR-013). Training staff on the IIS business continuity plan is critical to ensure quick response and implementation of the plan should a disruption occur. Response personnel should be fully educated on how to proceed in the event of a disruption. This includes thorough training on continuity options and resumption of normal operations. There is likely overlap with those who should be trained on the plan and those who assisted with developing the plan.

Developing and implementing a competency-based training and education curriculum that supports all individuals who have a role in the business continuity plan is vital for integrating the business continuity plan into practice.

Training should be administered via the most reasonable process for the jurisdiction. Some organizations with routine training programs for similar types of plans may incorporate training on the IIS business continuity plan. Training on the business continuity plan should be a part of new staff onboarding and included in job descriptions for those who have a role in maintaining or executing the plan. Training should be reviewed periodically and updated as the business continuity plan is updated. The training material should be clear and understandable to staff that was not involved with developing the business continuity plan.

In addition to routine training after development of the plan, it is important that just-in-time training can occur quickly should additional staff be needed to assist in response to a disruption. Short, computer-based modules may be an effective method of accomplishing this, although consideration should be given to having a nonelectronic version of training if the disruption affects the ability to use computer-based training. Emergency preparedness staff may have training materials that could be modified to fit this need. For additional access to training materials, consider storing a set of training materials at another location.

Another important component of training and education is comprehensive documentation throughout the development of the business continuity plan. If staff turnover occurs, this documentation shows how essential business functions were determined, why risk mitigation and continuity options were selected, and how other decisions were made. It is also important to document where copies of the plan exist. If updates are made to the plan, all copies of the plan and training materials should be updated.

5.3 EXERCISING THE PLAN

Once staff has been properly trained, it is important to exercise the business continuity plan on a regular basis to ensure that it is useful and practical and addresses needs of the program. Exercising the plan also helps augment training and provides an opportunity for improving the quality of the business continuity plan.

Exercising the plan can be accomplished in many ways, including by conducting tabletop exercises or full-scale exercises or by going through specific scenarios with inputs and discussing how the response in the plan addresses them.[29]

Once staff has been properly trained, it is important to exercise the business continuity plan on a regular basis to ensure that it is useful and practical and addresses needs of the program.

A full-scale exercise of the plan is conducted as though the disruption is occurring. Stakeholders and external partners may participate in the exercise, or programs may work with others in their region or programs that use the same IIS platform to conduct joint exercises. A smaller-scale exercise such as a tabletop exercise or an exercise of a specific aspect of the plan may still benefit from incorporation of outside partners (e.g., local public health staff input via telephone). These types of exercises also provide a good opportunity to use real-life examples to explore nuanced decisions, such as when to escalate an issue and when to implement a larger communication plan. Emergency preparedness staff may be a helpful resource as an appropriate exercise is determined.

The frequency of exercising the plan may depend on the type of exercise. For example, a tabletop exercise may be conducted on an annual basis, whereas a full-scale exercise will likely be done less frequently because of the time and resources involved. Exercising may also be conducted via modules, with previous exercises built upon as time and resources permit.

[29] For more information about types of preparedness exercises, please see https://www.ready.gov/business/testing/exercises.

Before starting an exercise, it is important to determine the scope of the exercise, staff members to be involved, and the roles and responsibilities of participants.[30] While a more robust exercise will provide better insight into how well the plan works, it might not be as feasible because of the greater time and resources needed to conduct a large-scale exercise. Availability of resources will affect what is or is not included in the scope of the exercise and the number of staff members that will be involved.

Exercises may focus on a specific scenario involving a risk to a selected essential business function, a particular resource or set of resources that are missing, or a specific continuity option. To conduct a scenario-based exercise, a detailed scenario should be developed that includes a realistic disruption and significant impact on one or more essential business functions. During the exercise, staff should walk through the response, identify what risk mitigation strategies would be useful, determine how to implement continuity options, and decide what communication strategies to use.

For all business continuity plan exercises, subject matter experts and individuals to facilitate and document the process should be included. Successful exercising of the plan requires a significant amount of preparation, so jurisdictions may consider incorporating this into emergency preparedness training or real-world experiences (e.g., telecommuting during inclement weather). It is also important to consider scenarios under regular staffing conditions and under staffing affected by a situation such as a pandemic.

After the exercise, a critical final step is to debrief about the exercise and document any insights that arise. If needed, revisions of the business continuity plan, mitigation strategies, continuity options, and the communication plan should be made at this time. Further training of staff may be needed based on updates to the plan or gaps identified as a result of the exercise.

[30] For more information on developing a roles and responsibilities chart, please see https://racichart.org/.

Regular review of and updates to the business continuity plan are critical components of a business continuity management system.

5.4 REGULAR REVIEW AND UPDATES

Regular review of and updates to the business continuity plan are critical components of a business continuity management system (PR-014). The frequency of these may vary depending on the needs and resources of the program. One person should be assigned to regularly review the business continuity plan.

IIS programs support many business functions and are continually adding new capabilities. As changes are made to existing functionality or new functions are implemented, the business continuity plan should be revisited. Risk mitigation strategies and business continuity options for existing selected essential business functions may be altered or enhanced as resources allow. Depending on available resources and the extent of new functionality, a new business impact analysis may be needed to determine any new essential business functions to incorporate into the business continuity plan. External changes, such as vendor or contract changes, may require updates to the business continuity plan. After updates are made, staff involved in responding to disruptions will need further training and education.

6

USING THE BUSINESS CONTINUITY PLAN DURING A DISRUPTION

6 USING THE BUSINESS CONTINUITY PLAN DURING A DISRUPTION

6.1 PLAN ACTIVATION

> An important part of a comprehensive business continuity management system is preparing staff on how to utilize the business continuity plan during a disruption.

Documented procedures should be in place to indicate when the IIS business continuity plan should be activated and who has the authority to activate it. Certain circumstances will always dictate activating the business continuity plan, while other situations may require a conversation among leadership and/or stakeholders to determine if the plan should be activated. Additional resources may be needed to initiate a response, and other areas of the agency may need to be engaged to ensure adequate staffing and resources are available to scale an appropriate response to the disruption.

Prior to taking action, the IIS program should assess the disruption to determine the most appropriate response. This response will always include efforts to resolve the disruption and may also include communicating with users and employing business continuity options to continue affected business functions. Generally, the response to a disruption should be initiated with the least resource-intensive option and proceed to progressively more resource-intensive options if the disruption worsens or the lesser resource-intensive options are not effective. However, in some situations, it may be prudent to initiate a more resource-intensive response right away if there are adequate resources and it is likely to be the most effective option. There may also be circumstances in which the best decision is to not implement a business continuity option at the time of the disruption because the issue may self-resolve in a short period of time or because of cost or resource constraints.

Prior to taking action, the IIS program should assess the disruption to determine the most appropriate response.

Documented procedures should be in place to indicate when the IIS business continuity plan should be activated and who has the authority to activate it.

The level of available resources may depend on the severity of the disruption, and continuity options should be scalable to accommodate varying levels of resources. Scalability may mean implementing a continuity option with a limited number of staff or a larger number of staff for a more robust response and having a range of continuity options available based on the amount of resources available. Consideration should also be given to how the IIS business continuity plan interacts with larger agency plans during a disruption that affects areas beyond the IIS program. The larger plan may include guidance on prioritization and resource allocation.

6.2 GENERAL STANDING-DOWN PROCEDURES

Procedures for standing down the response and resuming normal operations after the disruption is resolved should be documented. In Step 5.4 in Chapter 3 of the business continuity planning process, considerations are given to resumption of business functions. Based on the length and circumstances of the disruption, certain tasks may need to be completed for resumption of the business function(s), such as data entry into the IIS. In addition to the resumption of business functions, other components of a response (e.g., temporary work responsibilities, parallel processes for business functions for a limited time period) will need to be discontinued in a thoughtful way.

Procedures for standing down the response and resuming normal operations after the disruption is resolved should be documented.

Plans and procedures should be in place for IIS program staff who have been assigned to disruption-related activities to return to their roles. For a larger disruption and/or a disruption that lasts for an extended period of time, staff from other areas of the agency may be involved in the response. These staff members may play a role in standing-down procedures.

PRINCIPLES 7

7 PRINCIPLES

Principles reflect business guidelines, practices, or norms that we choose to follow. The following table contains principles for developing and implementing a business continuity plan.

PRINCIPLE	STATEMENT
PR-001 – Business Continuity Plan Content	A business continuity plan should address the following with respect to disruptions: - Prevention - Mitigation - Response - Continuity of operations - Resumption of normal operations
PR-002 – Security and Confidentiality	All business continuity plans should maintain applicable security and confidentiality requirements.
PR-003 – Maintain Data Integrity	A business continuity plan should ensure the integrity of all data maintained by an IIS that is impacted by a disruption.
PR-004 – Process to Follow Steps	Development of a business continuity plan should follow the steps in the order presented in the business continuity plan development process (Chapter 3 of this guide).
PR-005 – Leadership Commitment	Leadership should demonstrate commitment to the business continuity plan.
PR-006 – Sufficient Resources	Sufficient resources should be made available to develop, adopt, exercise, implement, and regularly review and update the business continuity plan.
PR-007 – Additional Leadership Communication	Ensure that internal partners are aware that the IIS program is developing a business continuity plan.
PR-008 – Jurisdiction Plans	The business continuity plan should inform, comply with, and not contradict other applicable plans in the jurisdiction.
PR-009 – Legal Framework	The business continuity plan should inform, comply with, and not contradict applicable legislation, policies, and regulatory requirements.
PR-010 – Critical Time Frames	Recovery time objective and recovery point objective should be set for each selected essential business function.
PR-011 – Risk Calculation	Risk should be analyzed in terms of consequences (impact) and likelihood (probability).

PRINCIPLE	STATEMENT
PR-012 – Financial Support	Finance and administrative procedures should be developed to support the business continuity plan before, during, and after a disruption.
PR-013 – Competency-Based Training	The IIS program should develop and implement a competency-based training and education curriculum that supports all individuals who have a role in the business continuity plan.
PR-014 – Regular Review and Update	A business continuity plan should be reviewed regularly and updated as necessary.

> "Knowledge of certain principles easily compensates for the knowledge of certain facts."
>
> — Claude Helvetius

APPENDICES

APPENDICES

APPENDIX A ACRONYMS AND ABBREVIATIONS

This appendix contains a list of acronyms and abbreviations used throughout the document. See Appendix D: Vocabulary and Domain Model for definitions of some of these acronyms and abbreviations.

ACRONYM/ABBREVIATION	FULL VERSION
AIRA	American Immunization Registry Association
BCM	Business Continuity Management
CDC	Centers for Disease Control and Prevention
CDS	Clinical Decision Support
COOP	Continuity of Operations
EDE	Electronic Data Exchange
EHR	Electronic Health Record
HANs	Health Alert Networks
ICE	Immunization Calculation Engine
IIS	Immunization Information System
IQIP	Immunization Quality Improvement for Providers
IT	Information Technology
MIROW	Modeling of Immunization Registry Operations Workgroup
MTPD	Maximum Tolerable Period of Disruption
NIP	National Immunization Program
PR	Principle
RPO	Recovery Point Objective
RTO	Recovery Time Objective
UI	User Interface
VFC	Vaccines for Children
VTrckS	Vaccine Tracking System (a CDC tool)

APPENDIX B SELECTED REFERENCES

This appendix contains references to general materials that discuss aspects of business continuity planning and practice.

- AIRA. AIRA Confidentiality and Privacy: Considerations for IIS. October 2016. https://repository.immregistries.org/resource/aira-confidentiality-and-privacy-considerations-for-iis/
- AIRA. Security Guidance Considerations for Immunization Information Systems. June 2017. https://repository.immregistries.org/resource/security-guidance-considerations-for-immunization-information-systems/
- Business Continuity Institute. Good practice guidelines 2013: A Guide to Global Good Practice in Business Continuity. 2013. Available through secure, member web portal.
- Business Continuity Management (BCM) Institute Glossary (BCMPedia). Retrieved March 27, 2019, from http://www.bcmpedia.org.
- CDC. Immunization Information System (IIS) Functional Standards. Retrieved May 10, 2019, from https://www.cdc.gov/vaccines/programs/iis/func-stds.html.
- CDC. Risk Communication website. Retrieved May 10, 2019, from https://www.cdc.gov/healthcommunication/risks/index.html.
- Department of Homeland Security. Ready.gov website. Retrieved May 10, 2019, from https://www.ready.gov/.
- Health and Human Services. Health Information Privacy website. Retrieved May 10, 2019, from https://www.hhs.gov/hipaa/index.html.
- International Organization for Standardization. ISO 22313:2012(E). Societal security – *Business continuity management systems – Guidance*. 2012. https://www.iso.org/standard/50050.html
- National Fire Protection Association. *National Fire Protection Association 1600 Standard on Continuity, Emergency, and Crisis Management.* 2019. https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1600
- National Institute of Standards and Technology. Contingency Planning Guide for Information Technology Systems. June 2002. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34.pdf
- National Institute of Standards and Technology. Contingency Planning Guide for Federal Information Systems. May 2010. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf
- The Office of Enterprise Technology, State of Minnesota. Glossary of Information Security Terms and Definitions, 2014-08-20. https://mn.gov/mnit/images/SEC_R_Glossary.pdf

APPENDIX C SCOPE

This appendix contains a detailed statement of the scope used to develop the business continuity topic. Chapter 1 contains a summary of the material contained in this appendix.

GENERAL

The scope of the MIROW IIS business continuity topic includes recommendations for IIS programs to develop and implement a business continuity plan for selected essential business functions supported by the IIS program. The essence of development for this topic is application of an established business continuity framework to IIS-supported selected essential business functions.

The guide includes recommendations for:

- Initiation of a business continuity planning process
- Assessment of threats for the organization overall
- Business impact analysis:
  - Examining business functions and the effect that a disruption might have upon them
  - Identifying essential business functions and associated resources
  - Determining important time frames
- Risk assessment: Examining the level of risk that exists for a specific resource needed to support a selected essential business function
- Risk mitigation strategies and business continuity options for selected essential business functions of IIS programs
- Communication related to developing and implementing a business continuity plan
- Education and training on and exercise (i.e., testing) of a business continuity plan
- Review and update of a business continuity plan
- Plan activation, standing down, and resumption of normal activities

FOCUS STATEMENT

Development of a guide with consensus-based best practice recommendations for an IIS program to deal with disruptive incidents that affect selected essential business functions.

While IIS programs depend significantly on IT, the focus is on sustaining continuous business operations as opposed to sustaining IT systems that support those business operations.

INTENTIONS

- To support business continuity for IIS program operations
- To ensure uniformity and sharing of best practices among IIS programs
    - An assumption is that there is enough commonality across IIS programs to produce a guide
- To provide recommendations that are applicable regardless of state or local requirements and/or standards

SCOPE STATEMENT

The essence of development for this topic is application of an established business continuity framework (e.g., as described by the ISO 22313:2012 standard) for business functions supported by the IIS program.

Breadth of these efforts: sustaining essential business functions during disruptive incidents

Including:

1. Identification of essential business functions
2. Identification of resources required for selected essential business functions
3. Assignment of critical time frames, such as RTO and RPO, for selected essential business functions
4. Risk analysis that estimates the level of a risk for each resource used by a selected essential business function
5. Identification of mitigation strategies that lower the exposure to risk or lower the probability or impact of a risk
6. Identification of continuity options for selected essential business functions
7. Description of roles and responsibilities of IIS and immunization program staff regarding business continuity planning
8. Recommendations for IIS business continuity plans
9. Recommendations for recovery activities and programs designed to return conditions to a level that is acceptable to the entity, as time permits
10. Recommendations for communication related to developing and implementing a business continuity plan
11. Recommendations for education and training on and exercise of a business continuity plan
12. Recommendations for review and update of a business continuity plan
13. Recommendations for plan activation, standing down, and resumption of normal activities

Excluding:

1. Planned system migration
2. Details of technology solutions
3. Prevention activities designed to avoid or stop an incident from occurring
4. Aspects of continuity related to life, property, and environment

EMPHASIZED PERSPECTIVES

Primary

a. IIS program
b. Immunization program
c. VFC program
d. Provider organizations

Secondary

a. AFIX/IQIP
b. Other agency areas (e.g., surveillance, emergency preparedness)
c. IIS vendor
d. EHR vendor
e. Jurisdiction/state IT services
f. Health information exchanges
g. General public/patient populations
h. Local health departments
i. Tribal jurisdictions and health departments

SCOPE OF INTEGRATION

An IIS business continuity plan should interface with, be compatible with, or coordinate with other relevant initiatives or systems. Examples of other relevant initiatives or systems are:

- State and program business continuity plans
- CDC's Vaccine Tracking System (VTrckS)
- EHRs
- Vendor agreements or contracts

APPENDIX D VOCABULARY AND DOMAIN MODEL

This appendix contains a vocabulary (i.e., agreed upon terms and definitions) captured in a domain model (Figure 4).

The business vocabulary and domain model ensure that all terminology and concepts that appear in the process description (Chapter 3) and principles (Chapter 7) are known and understood. See Appendix A: Acronyms and Abbreviations for quick reference to acronyms and abbreviations of these definitions used throughout the guide.

VOCABULARY

Alternative Process (Workaround) is a different way of doing something for a short period of time.

Business Continuity is the strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions to continue business operations at an acceptable predefined level.[31]

Business Continuity Management System is a part of an overall management system that establishes, implements, operates, monitors, reviews, maintains, and improves business continuity.[32]

Business Continuity Plan is the documented procedures that guide organizations to mitigate the impact of a disruption and to respond, recover, resume, and restore to a predefined level of operation following disruption.[33]

Business Function is a description of work that is performed to accomplish a business unit's responsibility.[34]

[31] ISO 22313:2012(E), *Societal security — Business continuity management systems — Guidance*

[32] ISO 22313:2012(E), *Societal security — Business continuity management systems — Guidance*

[33] Adapted from ISO 22313:2012(E), *Societal security — Business continuity management systems — Guidance*

[34] BCM Institute. Business Function. (2017, August 28). Retrieved March 27, 2019, from http://www.bcmpedia.org/wiki/Business_Function

Business Impact Analysis is the process of analyzing business functions and the effect that a disruption might have upon them.[35]

Communication is a process by which information is exchanged between individuals through a common system of symbols, signs, or behavior.[36]

Continuity Option is an alternative course of action, such as using an alternative process or relocation, for implementing a business function affected by a disruption.

Disruption is an interruption of normal business operations or processes that can range from short-term to longer-term unavailability.[37]

Essential Business Function is a business function that supports an IIS program's key products and services and, when interrupted, has significant negative impact on the well-being of the public and IIS staff, the IIS program's reputation, product or service quality, or the ability to meet legal and regulatory requirements.

Exercise is an instrument to train for, assess, practice, and improve performance and capabilities in a controlled environment.[38]

IIS Program is the staff and/or activities that focus primarily on maintaining and operating the IIS in support of immunization program activities.

Incident is an event that might be, or could lead to, a disruption, loss, emergency, or crisis.[39]

Maximum Tolerable Period of Disruption (MTPD) is the time it would take for adverse impacts, which might arise as a result of not providing a business function, to become unacceptable.[40] *Additional comment:* Like RTO, resumption of the business function can be achieved by an alternate process or through restarting normal operations.

Probability is a the chance that a given event will occur.[41]

Recovery Point Objective (RPO) is the point prior to a disruption to which information used by a business function must be restored to minimize the loss of data resulting from the disruption.

[35] Adapted from ISO 22313:2012(E), *Societal security — Business continuity management systems — Guidance*

[36] Merriam-Webster. Communication. (2019, April 23). Retrieved May 3, 2019 from https://www.merriam-webster.com/dictionary/communication

[37] BCM Institute. Disruption. (2015, December 27). Retrieved March 27, 2019, from http://www.bcmpedia.org/wiki/Disruption

[38] ISO 22313:2012(E), *Societal security — Business continuity management systems — Guidance*

[39] Adapted from ISO 22313:2012(E), *Societal security — Business continuity management systems — Guidance*

[40] Adapted from ISO 22313:2012(E), *Societal security — Business continuity management systems — Guidance*

[41] Adapted from Merriam-Webster. Probability. (2019, April 30). Retrieved May 3, 2019 from https://www.merriam-webster.com/dictionary/probability

Recovery Time Objective (RTO) is the period of time following a disruption within which a business function must be resumed.[42] Additional comments:

- The RTO is less than the time it would take for disruptions to a product/service or activity to become unacceptable (MTPD).
- Resumption of the service can be achieved by an alternate process or through restarting normal operations.

Relocation is the transfer of people or activities to another physical location.

Resources are the people, information and data, technology, buildings/worksites, communication systems, equipment, and utilities that an organization has to have available to operate.[43]

Risk is an effect of uncertainty on objectives.[44]

Risk Assessment is an overall process of risk identification, risk analysis, and risk evaluation.[45]

Risk Mitigation is the implemention of measures to lower the exposure to risk and lower the probability or impact of a risk.[46]

Service Delivery is a method of delivering a service offered by a business function.

Testing is a procedure for evaluation; a means of determining the presence, quality, or veracity of something.[47]

Threat is a potential cause of an unwanted incident, which may result in harm to individuals, a system or organization, the environment, or the community.[48] Additional comment: Some threats such as bad weather are more commonly referred to as "hazards."

Threat Assessment is an evaluation and description of the type, scope, and nature of events or actions that can result in adverse consequences to an organization or specific assets.[49]

Time Frame is a period of time, especially with respect to some action or project.[50]

[42] Adapted from ISO 22313:2012(E), *Societal security — Business continuity management systems — Guidance*

[43] Adapted from ISO 22313:2012(E), *Societal security — Business continuity management systems — Guidance*

[44] ISO 22313:2012(E), *Societal security — Business continuity management systems — Guidance*

[45] ISO 22313:2012(E), *Societal security — Business continuity management systems — Guidance*

[46] Adapted from BCM Institute. Risk Mitigation. (2017, August 23). Retrieved April 1, 2019, from http://www.bcmpedia.org/wiki/Risk_Mitigation

[47] ISO 22313:2012(E), *Societal security — Business continuity management systems — Guidance*

[48] ISO 22300:2012, *Societal security — Terminology*

[49] The Office of Enterprise Technology, State of Minnesota, Glossary of Information Security Terms and Definitions, 2014-08-20. https://mn.gov/mnit/images/SEC_R_Glossary.pdf

[50] Merriam-Webster. Time frame. (2019, April 21). Retrieved May 3, 2019, from https://www.merriam-webster.com/dictionary/timeframe

DOMAIN DIAGRAM

A domain model captures a business vocabulary (i.e., agreed-upon terms and definitions) in an illustrative manner (see Figure 4). The purpose of employing a domain model is to:

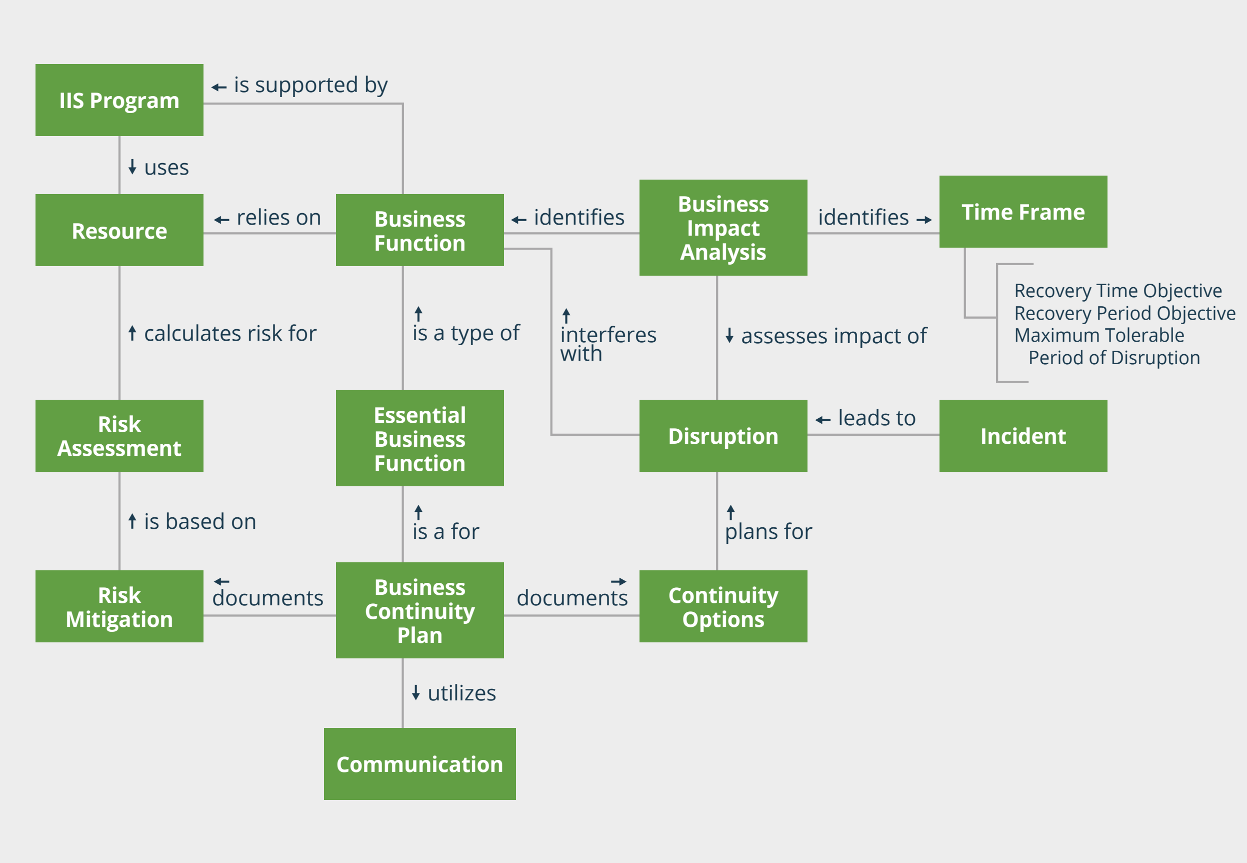
- Document agreed-upon terms and definitions for the project
- Facilitate discussions of the terms and definitions among project participants and provide tools to capture outcomes of these discussions
- Establish a foundation and a reference source (common vocabulary) for other project materials

How to read and interpret the domain diagram

- Relationships between terms are visualized by connecting lines.
- Names associated with these lines describe the types of relationships between terms.
  - For example, the relationship between **Business Function** and **Resource** is shown as a connecting line with the words **"relies on."** The relationship should be read as **"Business Function relies on Resource."**
  - The arrowhead "←" placed before the words **"relies on,"** which points to the **Resource**, indicates the direction in which to read the diagram (i.e., from **Business Function** to **Resource**).
  - To read the description in the opposite direction (i.e., from **Resource** to **Business Function**), a different phrase (i.e., "needed by") could be placed at the bottom of the line. The description would be **"Resource is needed by Business Function."**

For more information about domain diagrams and the vocabulary used in MIROW guides, please see *MIROW Common Vocabulary*, which serves as a glossary of terms so that the reader understands the common vocabulary used in all MIROW guides.

Figure 4 | *Business continuity domain diagram*



APPENDIX E TYPES OF CONTINUITY-RELATED PLANS[51]

There are many types of plans that support an organization in terms of security, continuity, preparedness, and recovery. Likewise, different terminology can be used to describe similar types of plans.

A list of types of plans from the National Institute of Standards and Technology (NIST) Contingency Planning Guide for Information Technology Systems is presented in this appendix. For more information about how an IIS business continuity plan can integrate with other plans, read Chapter 4.

PLAN	PURPOSE	SCOPE
Business Continuity Plan	Provide procedures for sustaining essential business operations while recovering from a significant disruption	Addresses business processes; IT is addressed based only on its support for business processes
Business Recovery (or Resumption) Plan	Provide procedures for recovering business operations immediately following a disaster	Addresses business processes; not IT-focused; IT addressed based only on its support for business processes
Continuity of Operations Plan (COOP)	Provide procedures and capabilities to sustain an organization's essential, strategic functions	Addresses the subset of an organization's missions that are deemed most critical; usually written at headquarters level; not IT-focused
Continuity of Support Plan/IT Contingency Plan	Provide procedures and capabilities for recovering a major application or general support system	Same as IT contingency plan; addresses IT system disruptions; not business-process-focused
Crisis Communications Plan	Provide procedures for disseminating status reports to personnel and the public	Addresses communications with personnel and the public; not IT-focused
Cyber Incident Response Plan	Provide strategies to detect, respond to, and limit consequences of malicious cyber incident	Focuses on information security responses to incidents affecting systems and/or networks
Disaster Recovery Plan	Provide detailed procedures to facilitate recovery of capabilities at an alternate site	Often IT-focused; limited to major disruptions with long-term effects
Occupant Emergency Plan	Provide coordinated procedures for minimizing loss of life or injury and protecting against property damage in response to a physical threat	Focuses on personnel and property particular to the specific facility; not based on business process or IT system functionality

[51] All information in this table is based on the National Institute of Standards and Technology (NIST) Contingency Planning Guide for Information Technology Systems.

APPENDIX F MILESTONES

This appendix contains a checklist of milestones for a project timeline and high-level activities that are part of the business continuity planning process.

Step 1.5 in Chapter 3 gives more information about how to incorporate these milestones into a business continuity project charter.

□ Create a project team.

□ Conduct background research on existing plans and legal, regulatory, and policy impacts.

□ Draft a project charter.

□ Obtain leadership approval to begin development of business continuity plan.

□ Review threats for the organization.

□ Identify business functions of IIS.

□ Determine and document selected essential business functions.

□ Assess risks for selected essential business functions.

□ Determine risk mitigation strategies for resources of selected essential business functions.

□ Identify continuity options for selected essential business functions.

□ Weigh value factors to decide which risk mitigation strategies and business continuity options to implement.

□ Identify resumption considerations.

□ Document the business continuity plan.

□ Obtain approval of the business continuity plan.

□ Conduct training and education for staff involved in response.

□ Ensure regular exercising and review of the business continuity plan.

APPENDIX G EXAMPLE TABLE TO IDENTIFY POTENTIAL ESSENTIAL BUSINESS FUNCTIONS

Step 3.2 in Chapter 3 describes a process to identify the business functions that are essential to the IIS program, using the list of business functions that was developed in Step 3.1 in Chapter 3.

The five factors listed below can be used to determine which business functions are considered potential essential business functions. IIS programs can determine if other factors should be considered in this process. Likewise, IIS programs can determine if factors should have equal weight or differing weights based on their importance. The IIS program should develop a table to record a "score" for each factor for each business function. An example of a table is included below.

FACTORS TO DETERMINE ESSENTIAL BUSINESS FUNCTIONS	VACCINE ORDERING CAPABILITY	CDS FOR EVALUATING IMMUNIZATION HISTORY	REMINDER/RECALL
Time Critical 1 (low) – 3 (high)	3	3	1
Legal Requirement 1 (low) – 3 (high)	1	1	1
Health and Safety 1 (low) – 3 (high)	2	3	1
Customer Impact 1 (low) – 3 (high)	3	3	1
Reputation 1 (low) – 3 (high)	2.5	3	1
Total Score	11.5	13	5

APPENDIX H EXAMPLE OF SELECTED ESSENTIAL BUSINESS FUNCTIONS IDENTIFIED BY THE WORKGROUP

> As described in Task 3 in Chapter 3 of the guide, one of the steps in development of a business continuity plan is to perform a business impact analysis.

Business impact analysis is the process of analyzing IIS program operational functions and the effect that a disruption might have upon them. The purpose of a business impact analysis is to determine the essential business functions of the IIS program and prioritize essential business functions to focus business continuity planning. The Business Continuity Workgroup (see Appendix V for list of participants) went through the process described in Task 3 in Chapter 3 to identify a list of selected essential business functions.

METHODOLOGY

The small group developed a proposed list of IIS program essential business functions based on:

- Review and analysis of IIS Functional Standards
- Feedback from the MIROW Steering Committee
- Feedback from IIS community volunteers who responded to a survey and/or a telephone interview
- Consideration of upstream dependencies (Step 3.3 in Chapter 3 and Appendix I)

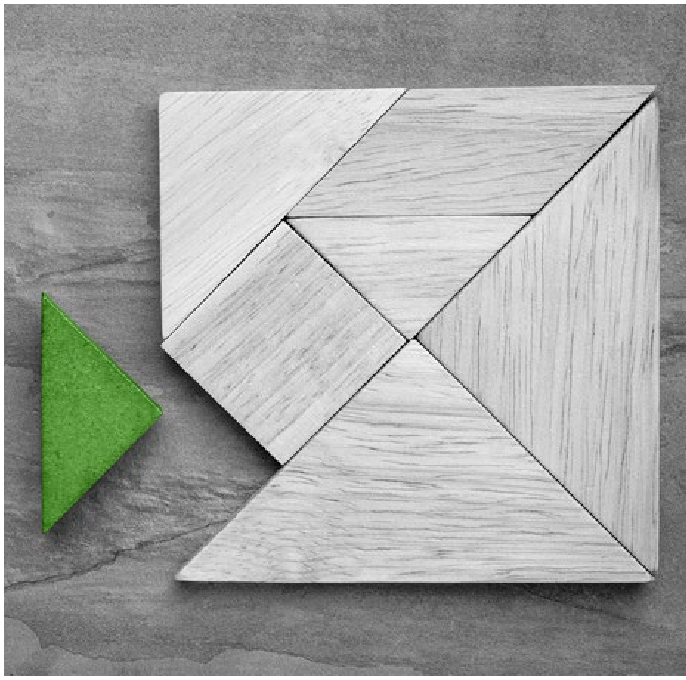
The small group divided the proposed IIS program essential business functions into two broad categories:

- **Externally facing essential business functions:** Work that is performed to accomplish responsibilities of the IIS program to outside stakeholders.
- **Supporting essential business functions:** Work that is performed by the IIS program internally that underpins IIS program operations and supports more than one of the externally facing business functions. Supporting essential business functions are related to the IIS Essential Infrastructure Functional Standards v4.0. This project focused on externally facing essential business functions; however, an IIS program may determine that it wants to include supporting essential business functions in its business continuity plan.

SELECTED ESSENTIAL BUSINESS FUNCTIONS IDENTIFIED BY THE BUSINESS CONTINUITY WORKGROUP

Based on the preparatory work of the small group, the Business Continuity Workgroup identified seven externally facing selected essential business functions to assist in development of a business continuity plan. The selected essential business functions identified by the Business Continuity Workgroup are as follows (presented in alphabetical order):

- Accepting immunization and demographic information
- Providing access to demographic information and immunization history for clinical purposes
- Providing clinical decision support for evaluation of patient immunization history
- Providing clinical decision support for forecasting doses due
- Providing help desk support
- Providing vaccine ordering capability
- Supporting outbreak investigation



BEST PRACTICE RECOMMENDATION

Each IIS program should combine use of:

- The process recommended in Task 3 in Chapter 3 to identify selected essential business functions
- The list of selected essential business functions developed by the Business Continuity Workgroup

Each IIS program should use one of the following options to implement the best practice recommendation:

- **Option 1:** Follow the process recommended in Task 3 in Chapter 3 to identify selected essential business functions for the IIS program. Compare the resulting essential business functions with the list of selected essential business functions identified by the Business Continuity Workgroup to identify, discuss, and confirm or adjust discrepancies.
- **Option 2:** Begin with the list of selected essential business functions identified by the Business Continuity Workgroup. Adjust the list based on circumstances of the IIS program, referencing the guidance and criteria in Task 3 in Chapter 3.

The final list of essential business functions included in a business continuity plan is dependent on the time and resources available.

APPENDIX I EXAMPLE ILLUSTRATIONS OF UPSTREAM DEPENDENCIES

As described in Step 3.3 in Chapter 3, once potential essential business functions have been identified, the next step is to determine the upstream dependencies associated with them.

Upstream dependencies are the activities/processes that must occur for the potential essential business function to operate. The process of identifying upstream dependencies may highlight additional potential essential business functions that were not previously identified. For example, if a business function is an upstream dependency for several potential essential business functions, it may also be a potential essential business function. An illustration of this step is presented below.

To develop examples of tools that can be used for business continuity plan development, the workgroup used three business functions as examples throughout the appendices:

- Providing vaccine ordering capability
- Providing access to demographic information and immunization history for clinical purposes — via direct user interface (UI) or electronic data exchange (EDE)
- Providing clinical decision support (CDS) for evaluation of patient immunization history — via direct UI or EDE

These are shortened to better fit into tables and figures:

- Vaccine ordering capability
- Access to demographic information and immunization history
- CDS for evaluation of patient immunization history

Figure 5 | *Upstream dependency illustration – vaccine ordering capability*

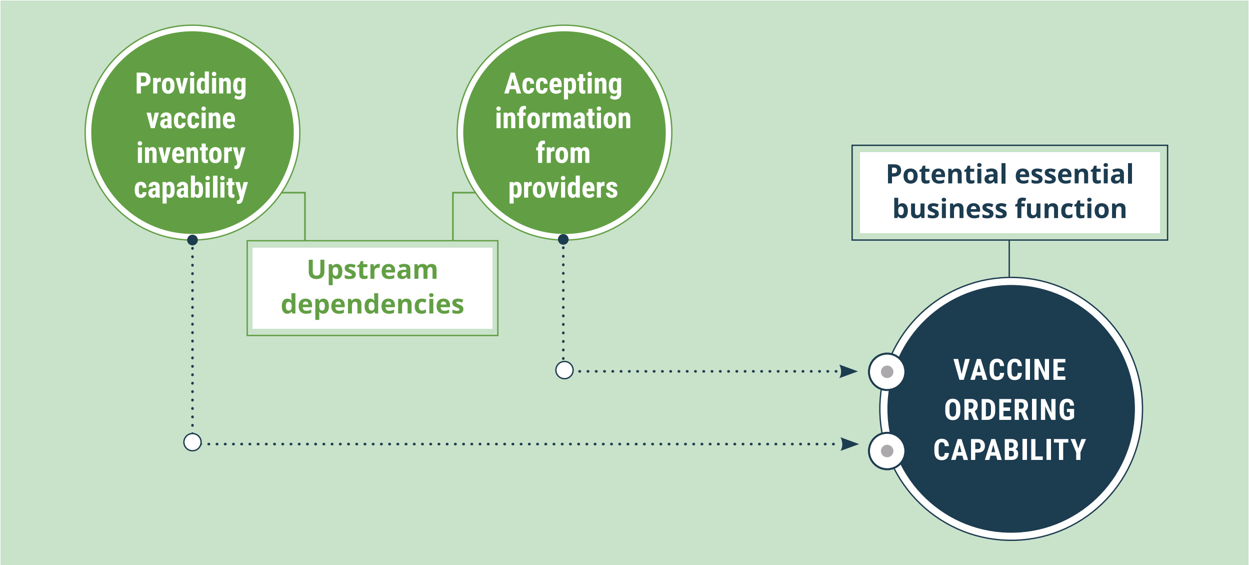

Providing vaccine inventory capability
Accepting information from providers
Upstream dependencies
Potential essential business function
VACCINE ORDERING CAPABILITY

Figure 6 | *Upstream dependency illustration – CDS for evaluation of patient immunization history*

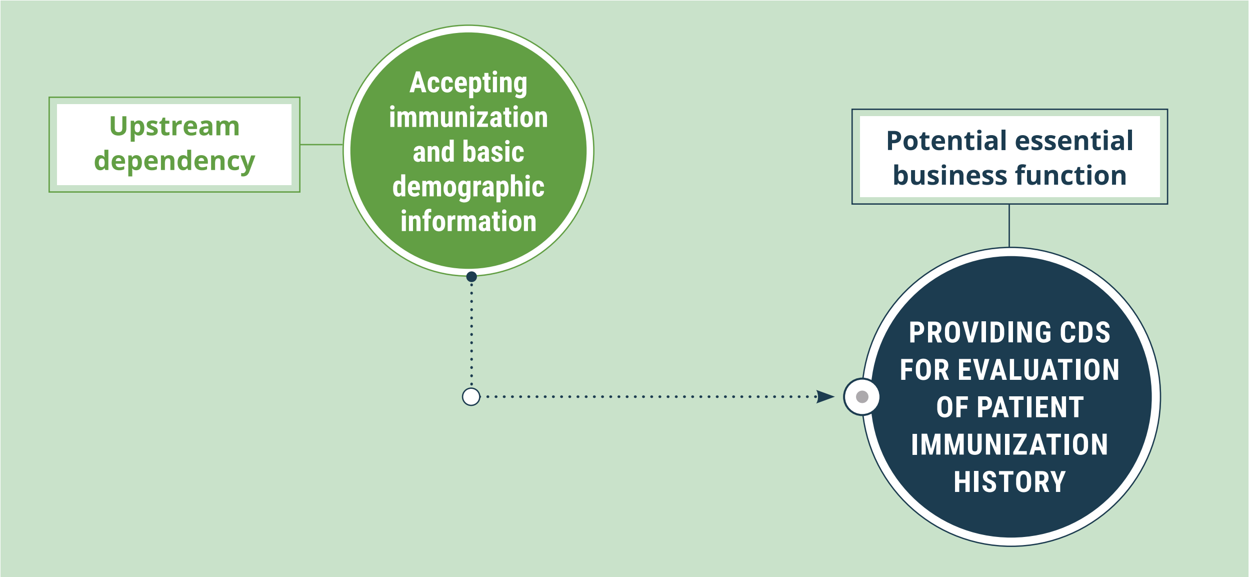
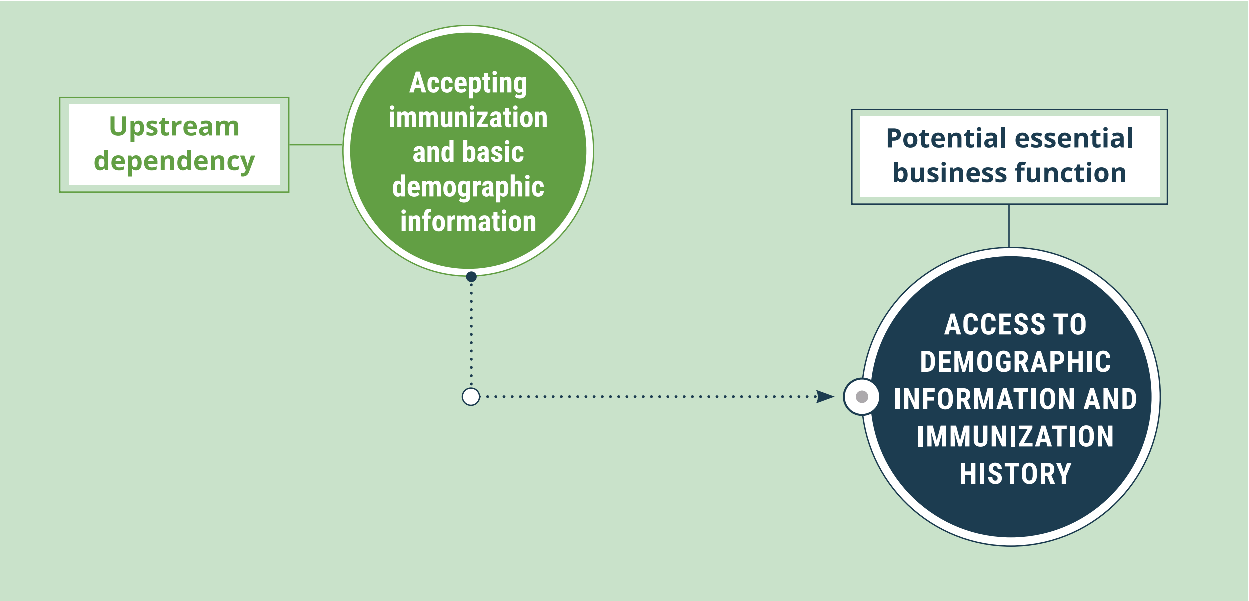

Upstream dependency
Accepting immunization and basic demographic information
Potential essential business function
PROVIDING CDS FOR EVALUATION OF PATIENT IMMUNIZATION HISTORY

Figure 7 | *Upstream dependency illustration – access to demographic information and immunization history*


Upstream dependency
Accepting immunization and basic demographic information
Potential essential business function
ACCESS TO DEMOGRAPHIC INFORMATION AND IMMUNIZATION HISTORY

APPENDIX J EXAMPLE USE CASES

> As described in Step 3.4 in Chapter 3, the IIS program should develop a use case to document the normal operations for each selected essential business function.

This appendix includes the three examples of selected essential business functions used in Appendix I in two use cases:

- A use case for vaccine ordering capability.
- A use case that combines access to demographic information and immunization history and CDS for evaluation of patient immunization history. These two example business functions were combined because the workgroup found that the processes significantly overlapped, thus creating very similar use cases. While the example selected essential business functions have been combined, there are two separate use cases that address performing these two business functions via direct UI and EDE.

Use case for vaccine ordering capability

	PROCESS STEP	NORMAL ("SUNNY DAY") SCENARIO
1	Provider organization staff submits a vaccine order to the awardee vaccine program.	**Activities:** Provider organization logs into the IIS via direct UI. Provider organization accesses ordering screen(s). Provider organization enters ordering information (orders, provider inventory, provider master data). Provider organization also enters additional information required by the vaccine program (e.g., information about temperature excursions in storage units). Provider organization verifies the information is correct (e.g., delivery hours and contact information).
2	Awardee vaccine program ordering staff approves the vaccine order.	**Activities:** Ordering staff logs into the IIS via direct UI. Ordering staff reviews additional information required by the vaccine program prior to approving the order. Ordering staff reviews, edits, and approves the order.

	PROCESS STEP	NORMAL ("SUNNY DAY") SCENARIO
3	Awardee vaccine program ordering staff submits the vaccine order to VTrckS.	**Activities:** Ordering staff exports the three files from the IIS into a desktop folder. Ordering staff logs into VTrckS and uploads files to VTrckS.
4	VTrckS validates and accepts the vaccine order.	**Activities:** VTrckS conducts internal checks.
5	Awardee vaccine program ordering staff gets information about the vaccine order fulfillment. Use case ends.	**Activities:** Ordering staff logs into VTrckS to download the shipment information for the vaccine order and uploads it into the IIS. This is a daily activity, with no notification.

Use case for access to demographic information and immunization history and CDS for evaluation of patient immunization history – direct UI

	NORMAL ("SUNNY DAY") SCENARIO	NORMAL ("SUNNY DAY") SCENARIO
1	Provider organization assembles patient identifying information.	**Activities:** Provider organization obtains patient identifying information needed to request the patient's information from the IIS direct UI. For example, a provider asks a patient for identifying information or pulls a patient's medical chart.
2	Provider organization submits request for patient's demographic and immunization information to the IIS.	**Activities:** Provider organization logs into the IIS via direct UI and enters patient's identifying information into the IIS via direct UI screen(s) using a search screen.
3	IIS assembles response information consisting of patient demographic information and patient immunization history.	**Activities:** IIS assembles patient demographic information and patient immunization history.
4	IIS evaluates patient's immunization history and augments response information with evaluation results (valid/invalid doses).	**Activities:** IIS evaluates patient immunization history and augments it with valid/invalid designation for vaccine doses.
5	IIS evaluates patient immunization history portion of the response and augments it with recommended vaccine doses.	**Activities:** IIS evaluates patient immunization history and augments it with recommended vaccine doses.

	NORMAL (“SUNNY DAY”) SCENARIO	NORMAL (“SUNNY DAY”) SCENARIO
6	IIS submits response information to the provider organization.	**Activities:** IIS presents patient demographic information and patient immunization history on direct UI screen(s).
7	Provider organization receives and utilizes response from IIS. Use case ends.	**Activities:** Provider organization reads patient demographic information and patient immunization history on direct UI screen(s) and utilizes that information.

Use case for access to demographic information and immunization history and CDS for evaluation of patient immunization history – EDE

	PROCESS STEP	NORMAL (“SUNNY DAY”) SCENARIO
1	Provider organization assembles patient identifying information.	**Activities:** Provider organization, using an EHR system, constructs an appropriately formatted and populated query that contains the patient’s identifying information and provider organization information.
2	Provider organization submits request for patient’s demographic and immunization information to the IIS.	**Activities:** Provider organization, using an EHR, submits a query to an IIS as an electronic message for patient demographic information and patient immunization history.
3	IIS assembles response information consisting of patient demographic information and patient immunization history.	**Activities:** IIS constructs an appropriately formatted and populated response that contains patient demographic information and patient immunization history.
4	IIS evaluates patient’s immunization history and augments response information with evaluation results (valid/invalid doses).	**Activities:** IIS evaluates patient immunization history portion of the response and augments it with valid/invalid designation for vaccine doses.
5	IIS evaluates patient immunization history portion of the response and augments it with recommended vaccine doses.	**Activities:** IIS evaluates patient immunization history portion of the response and augments it with recommended vaccine doses.
6	IIS submits response information to the provider organization.	**Activities:** IIS submits response (as an electronic message) to provider organization.
7	Provider organization receives and utilizes response from IIS. Use case ends.	**Activities:** Provider organization, using the EHR, receives and utilizes response (electronic message) from IIS.

APPENDIX K EXAMPLE USE CASES WITH RESOURCES

As described in Step 3.4.1 in Chapter 3, after identifying a selected essential business function, the next step is to identify the resources needed to support the function's normal operations.

The use cases that were developed in Step 3.4 in Chapter 3 can help identify the resources needed for the selected essential business function. This appendix gives examples of resources needed to support the three examples of selected essential business functions. Like in Appendix J, this appendix combines the example selected essential business functions of access to demographic information and immunization history and CDS for evaluation of patient immunization history. There are two separate use cases that address performing these two business functions via direct UI and EDE.

Use case for vaccine ordering capability with resources

	PROCESS STEP	NORMAL ("SUNNY DAY") SCENARIO	RESOURCES
1	Provider organization staff submits a vaccine order to the awardee vaccine program.	**Activities:** Provider organization logs into the IIS via direct UI. Provider organization accesses ordering screen(s). Provider organization enters ordering information (orders, provider inventory, provider master data). Provider organization also enters additional information required by the vaccine program (e.g., information about temperature excursions in storage units). Provider organization verifies the information is correct (e.g., delivery hours and contact information).	**People:** Provider organization vaccine coordinator and backup coordinator **Information and Data:** Provider's inventory, the order itself, supporting documentation, including temperature logs and provider demographics **Technology:** IIS, EHR **Communication:** Internet **Equipment:** Provider organization computer **Building:** Provider facility **Utilities:** Electricity

	PROCESS STEP	NORMAL ("SUNNY DAY") SCENARIO	RESOURCES
2	Awardee vaccine program ordering staff approves the vaccine order.	**Activities:** Ordering staff logs into the IIS via direct UI. Ordering staff reviews additional information required by the vaccine program prior to approving the order. Ordering staff reviews, edits, and approves the order.	**People:** Awardee ordering staff and backup Information and Data: Provider's inventory, the order itself, supporting documentation, including temperature logs and provider demographics **Technology:** IIS **Communication:** Internet **Equipment:** Ordering staff computer **Building:** IIS program facility **Utilities:** Electricity
3	Awardee vaccine program ordering staff submits the vaccine order to VTrckS.	**Activities:** Ordering staff exports the three files from the IIS into a desktop folder. Ordering staff logs into VTrckS and uploads files to VTrckS.	**People:** Awardee ordering staff and backup **Information and Data:** Required VTrckS files (orders, provider inventory, provider master data) **Technology:** IIS, VTrckS **Communication:** Internet **Equipment:** Ordering staff computer **Building:** IIS program facility **Utilities:** Electricity
4	VTrckS validates and accepts the vaccine order.	**Activities:** VTrckS conducts internal checks.	**Information and Data:** Required VTrckS files (orders, provider inventory, provider master data) **Technology:** VTrckS **Communication:** Internet **Utilities:** Electricity
5	Awardee vaccine program ordering staff gets information about the vaccine order fulfillment. Use case ends.	**Activities:** Ordering staff logs into VTrckS to download the shipment information for the vaccine order and uploads into the IIS. This is a daily activity, with no notification.	**People:** Awardee ordering staff and backup **Information and Data:** Shipment information **Technology:** IIS, VTrckS **Communication:** Internet **Equipment:** Ordering staff computer **Building:** IIS program facility **Utilities:** Electricity

Use case for access to demographic information and immunization history and CDS for evaluation of patient immunization history with resources – direct UI

	PROCESS STEP	NORMAL ("SUNNY DAY") SCENARIO	RESOURCES
1	Provider organization assembles patient identifying information.	**Activities:** Provider organization obtains patient identifying information needed to request the patient's information from the IIS direct UI. For example, a provider asks a patient for identifying information or pulls a patient's medical chart.	**People:** Provider organization staff (i.e., authenticated user) **Information and Data:** Patient demographic information, provider organization information **Technology:** EHR **Communication:** Internet **Equipment:** Provider organization computer **Building:** Provider facility **Utilities:** Electricity
2	Provider organization submits request for patient's demographic and immunization information to the IIS.	**Activities:** Provider organization logs into the IIS via direct UI and enters patient's identifying information into the IIS via direct UI screen(s) using a search screen.	**People:** Provider organization staff **Information and Data:** Patient demographic information, provider organization information **Technology:** IIS **Communication:** Internet **Equipment:** Provider organization computer **Building:** Provider facility **Utilities:** Electricity
3	IIS assembles response information consisting of patient demographic information and patient immunization history.	**Activities:** IIS assembles patient demographic information and patient immunization history.	**Information and Data:** Patient demographic information and patient immunization history **Technology:** IIS **Communication:** Internet **Utilities:** Electricity
4	IIS evaluates patient's immunization history and augments response information with evaluation results (valid/invalid doses).	**Activities:** IIS evaluates patient immunization history and augments it with valid/invalid designation for vaccine doses.	**Information and Data:** Evaluated patient immunization history **Technology:** IIS, internal or stand-alone CDS **Communication:** Internet **Utilities:** Electricity

	PROCESS STEP	NORMAL ("SUNNY DAY") SCENARIO	RESOURCES
5	IIS evaluates patient immunization history portion of the response and augments it with recommended vaccine doses.	**Activities:** IIS evaluates patient immunization history and augments it with recommended vaccine doses.	**Information and Data:** Recommended vaccine doses **Technology:** IIS, internal or stand-alone CDS **Communication:** Internet **Utilities:** Electricity
6	IIS submits response information to the provider organization.	**Activities:** IIS presents patient demographic information and patient immunization history on direct UI screen(s).	**Information and Data:** Patient demographic information, patient immunization history, recommended vaccine doses **Technology:** IIS **Communication:** Internet **Utilities:** Electricity
7	Provider organization receives and utilizes response from IIS. Use case ends.	**Activities:** Provider organization reads patient demographic information and patient immunization history on direct UI screen(s) and utilizes that information.	**People:** Provider organization staff **Information and Data:** Patient demographic information, patient immunization history, recommended vaccine doses **Technology:** IIS **Communication:** Internet **Equipment:** Provider organization computer **Building:** Provider facility **Utilities:** Electricity

Use case for access to demographic information and immunization history and CDS for evaluation of patient immunization history with resources – EDE

	PROCESS STEP	NORMAL ("SUNNY DAY") SCENARIO	RESOURCES
1	Provider organization assembles patient identifying information.	**Activities:** Provider organization, using an EHR system, constructs an appropriately formatted and populated query that contains the patient's identifying information and provider organization information.	**People:** Provider organization staff **Information and Data:** Patient demographic information, provider organization information **Technology:** EHR **Communication:** Internet **Equipment:** Provider organization computer **Building:** Provider facility **Utilities:** Electricity

	PROCESS STEP	NORMAL ("SUNNY DAY") SCENARIO	RESOURCES
2	Provider organization submits request for patient's demographic and immunization information to the IIS.	**Activities:** Provider organization, using an EHR, submits a query to an IIS as an electronic message for patient demographic information and patient immunization history.	**People:** Provider organization staff **Information and Data:** Patient demographic information, provider organization information **Technology:** EHR, IIS **Communication:** Internet, transport protocol **Equipment:** Provider organization computer **Building:** Provider facility **Utilities:** Electricity
3	IIS assembles response information consisting of patient demographic information and patient immunization history.	**Activities:** IIS constructs an appropriately formatted and populated response that contains patient demographic information and patient immunization history.	**Information and Data:** Patient demographic information, patient immunization history **Technology:** IIS **Communication:** Internet **Utilities:** Electricity
4	IIS evaluates patient's immunization history and augments response information with evaluation results (valid/invalid doses).	**Activities:** IIS evaluates patient immunization history portion of the response and augments it with valid/invalid designation for vaccine doses.	**Information and Data:** Evaluated patient immunization history **Technology:** IIS, internal or stand-alone CDS **Communication:** Internet **Utilities:** Electricity
5	IIS evaluates patient immunization history portion of the response and augments it with recommended vaccine doses.	**Activities:** IIS evaluates patient immunization history portion of the response and augments it with recommended vaccine doses.	**Information and Data:** Recommended vaccine doses **Technology:** IIS, internal or stand-alone CDS **Communication:** Internet **Utilities:** Electricity
6	IIS submits response information to the provider organization.	**Activities:** IIS submits response (as an electronic message) to provider organization.	**Information and Data:** Patient demographic information, patient immunization history, recommended vaccine doses **Technology:** IIS **Communication:** Internet **Utilities:** Electricity
7	Provider organization receives and utilizes response from IIS. Use case ends.	**Activities:** Provider organization, using the EHR, receives and utilizes response (electronic message) from IIS.	**People:** Provider organization staff **Information and Data:** Patient demographic information, patient immunization history, recommended vaccine doses **Technology:** IIS, EHR **Communication:** Internet **Equipment:** Provider organization computer **Building:** Provider facility **Utilities:** Electricity

APPENDIX L EXAMPLE RESOURCE TABLES

As described in Step 3.4.1, once the resources needed to support each essential business function have been identified, incorporate them into a table to allow for quick reference and comparison of resources.

The broad resource categories to consider are:

- People
- Information and data
- Technology
- Communications systems
- Equipment, buildings/worksites
- Utilities

The tables in this appendix illustrate various ways to organize the presentation of resources needed to support the three examples of selected essential business functions. Like in previous appendices, this appendix combines the example selected essential business functions of access to demographic information and immunization history and CDS for evaluation of patient immunization history. There are two separate rows that address performing these two business functions via direct UI and EDE.

Resource table for use cases

ESSENTIAL BUSINESS FUNCTION	PEOPLE	INFORMATION AND DATA	TECHNOLOGY	COMMUNICATION SYSTEMS	EQUIPMENT	BUILDINGS/ WORKSITES	UTILITIES
Vaccine ordering capability	• Provider organization vaccine coordinator and backup coordinator • Awardee ordering staff and backup	• Provider's inventory, the order itself, supporting documentation, including temperature logs, provider demographics • Required VTrckS files (order, provider inventory, provider master data) • Shipment information	• IIS • EHR • VTrckS	• Internet	• Provider's computer • Ordering staff's computer	• IIS program facility • Provider facility	• Electricity
Access to demographic information and immunization history and CDS for evaluation of patient immunization history with resources – UI	• Provider organization staff	• Patient demographic information, provider organization information • Patient immunization history • Evaluated patient immunization history • Recommended vaccine doses	• EHR • IIS • CDS	• Internet	• Provider organization computer	• Provider facility	• Electricity
Access to demographic information and immunization history and CDS for evaluation of patient immunization history with resources – EDE	• Provider organization staff	• Patient demographic information, provider organization information • Patient immunization history • Evaluated patient immunization history • Recommended vaccine doses	• EHR • IIS • CDS	• Internet • Transport protocol	• Provider organization computer	• Provider facility	• Electricity

Resources by category: vaccine ordering capability

RESOURCE TYPE	SPECIFIC RESOURCE(S)
People	Vaccine coordinator and backup at provider site
	Awardee ordering staff and backup
Information and data	Provider's order
	Supporting information from provider
	Required VTrckS files (orders, inventory, provider master data)
	Shipment information
Equipment	Provider's computer
	Ordering staff's computer
Technology	IIS
	EHR
	VTrckS
Communication Systems	Internet
Building/Worksite	Provider facility
	IIS program facility
Utilities	Electricity

Resources by category: access to demographic information and immunization history and CDS for evaluation of patient immunization history with resources

RESOURCE TYPE	SPECIFIC RESOURCE(S)
People	Provider organization staff
Information and data	Patient demographic information
	Patient immunization history
	Evaluated patient immunization history
	Recommended vaccine doses
Equipment	Provider organization computer
Technology	EHR
	IIS
	CDS
Communication Systems	Internet
	Transport protocol (EDE only)
Building/Worksite	Provider facility
Utilities	Electricity

APPENDIX M EXAMPLE CRITICAL TIME FRAME TABLE

As discussed in Step 3.4.2 in Chapter 3, an option for comparing the critical time frames of multiple selected essential business functions is to develop a critical time frame table.

This table can be helpful in providing a quick visual reference for IIS staff and leadership about the time frames involved with business continuity for the IIS program.

	0–24 HOURS	24 HOURS–1 WEEK	1 WEEK–1 MONTH	GREATER THAN 1 MONTH
BUSINESS FUNCTION				
Business Function One	🟨	🟧	🟥	🟥
Business Function Two	🟩	🟨	🟥	🟥
Business Function Three	🟩	🟩	🟨	🟨
Business Function Four	🟩	🟩	🟨	🟨
Business Function Five	🟩	🟩	🟨	🟥
Business Function Six	🟩	🟩	🟨	🟧
Business Function Seven	🟩	🟩	🟩	🟨

KEY
🟩 Low risk of negative impact
🟨 Medium risk of negative impact
🟧 High risk of negative impact
🟥 Very high risk of negative impact

APPENDIX N EXAMPLE TABLES FOR CALCULATING RISK FOR RESOURCES BY SELECTED ESSENTIAL BUSINESS FUNCTION

As described in Task 4 in Chapter 3, after identifying the resources for each selected essential business function, the next step is to calculate the risk for each resource used.

Risk should be analyzed in terms of consequences (impact) and likelihood (probability) of each resource for each selected essential business function. This appendix contains examples of tables that can be used for scoring resources for the three examples of selected essential business functions. Like in previous appendices, this appendix combines the example selected essential business functions of access to demographic information and immunization history and CDS for evaluation of patient immunization history.

Scale: 1 (low) to 10 (high)

Calculating risk for vaccine ordering capability

SPECIFIC RESOURCE(S)	PROBABILITY	IMPACT	CALCULATED RISK	RESPONSIBLE PARTY
Vaccine coordinator and backup at provider site	1	10	10	Provider
Awardee ordering staff and backup	4	10	40	IIS program/agency
Provider's order	1	10	10	Provider
Supporting information from provider	1	5	5	Provider
Required VTrckS files (orders, inventory, provider master data)	3	10	30	IIS
Shipment information	4	2	8	CDC/McKesson
Provider's computer	2	10	20	Provider
Ordering staff's computer	3	10	30	IIS program/agency

SPECIFIC RESOURCE(S)	PROBABILITY	IMPACT	CALCULATED RISK	RESPONSIBLE PARTY
IIS (ordering functionality)	5	10	50	IIS program/agency/ vendor
EHR	2	2	4	EHR vendor/provider
VTrckS	6	10	60	CDC
Internet	5	10	50	Agency IT, provider IT
Provider facility	1	10	10	Provider
IIS program facility	2	3	6	Agency
Electricity	4	10	40	Power company

Calculating risk for access to demographic information and immunization history and CDS for evaluation of patient immunization history with resources

SPECIFIC RESOURCE(S)	PROBABILITY	IMPACT	CALCULATED RISK	RESPONSIBLE PARTY
Provider organization staff	1	10	10	Provider
Patient demographic information	1	10	10	Provider
Patient immunization history	1	10	10	Provider
Evaluated patient immunization history	3	10	30	IIS program/agency
Recommended vaccine doses	3	10	30	IIS program/agency
Provider's computer	1	10	10	Provider
EHR	1	10	10	Provider
IIS	3	10	30	IIS program/agency/vendor
CDS	3	10	30	IIS program/agency/vendor
Internet	5	10	50	Agency IT, provider IT
Transport protocol (EDE only)	2	10	20	IIS program
Provider facility	1	10	10	Provider
Electricity	4	10	40	Power company

APPENDIX O EXAMPLE TABLES FOR IDENTIFYING RISK MITIGATION STRATEGIES

As described in Step 5.1 in Chapter 3, use the subset of resources (by selected essential business function) that are considered most important to address from Task 4 in Chapter 3 and develop risk mitigation strategies that would either decrease the probability of the resource being disrupted or decrease the impact if the resource is disrupted.

This appendix contains examples of tables with risk mitigation strategies for the three examples of selected essential business functions.

Possible risk mitigation strategies for vaccine ordering capability

RESOURCE	SPECIFIC RESOURCE	RISK MITIGATION
People	Vaccine coordinator and backup at provider site	• Training for staff about roles and cross-training • Providers' vaccine management plan
Technology	VTrckS	• Ensure providers always have six- to eight-week supply of vaccine on hand
Technology	IIS ordering functionality	• Keep up-to-date paper order form so that it's ready if needed • Ensure the process is documented • Ensure providers have a six- to eight-week supply of vaccine on hand • Regular system maintenance and system testing upon upgrade
People	Awardee ordering staff and backup	• Documenting standard operating procedures • Cross-training of staff
Utilities	Electricity	• Backup generator available to support the IIS and IIS program

Possible risk mitigation strategies for access to demographic information and immunization history using EDE

RESOURCE	SPECIFIC RESOURCE	RISK MITIGATION
Information and Data	Patient demographic information (provider)[52]	• Advise providers to have standard operating procedures and a continuity plan • IIS capable of sending error messages back to EHR • Providers have process in place to monitor errors and fix them • Have documentation in place for providers to know how to interpret error messages • Good onboarding of providers
Information and Data	Provider organization information (from provider)	• Advise providers to have standard operating procedures and a continuity plan • IIS capable of sending error messages back to EHR • Providers have process in place to monitor errors and fix them • Have documentation in place for providers to know how to interpret error messages • Good onboarding of providers
Information and Data	Patient immunization history (IIS)	• Regular maintenance and testing • Documentation of procedures • Cross-training/bench strength of IIS staff
Technology	IIS	• Regular maintenance and testing • Standard operating procedures • Monitoring tool in place that sends notifications if interface isn't working • Vendor contract service-level agreement; encourage vendor or internal IT to have processes in place • Cross-training/bench strength of IIS staff
Technology	CDS (internal or stand-alone)	• Maintenance and testing • Standard operating procedures • Monitoring tool in place that sends notifications if interface isn't working • Vendor contract; encourage vendor or internal IT to have processes in place, expectations of what happens if disrupted • Cross-training/bench strength of IIS staff

[52] Assumption that it's properly formatted but not received

Possible risk mitigation strategies for CDS for evaluation of patient immunization history using EDE

RESOURCE	SPECIFIC RESOURCE	RISK MITIGATION
Information and Data	Patient demographic information (from provider)	• Onboarding and training • Monitoring submissions and providing regular feedback to user
Information and Data	Provider organization information (from provider)	• Onboarding and training • Monitoring submissions and providing regular feedback to user
Information and Data	Patient immunization history (from IIS)	• Promoting reporting (including historical doses) • Regular system maintenance and testing • Data quality activities (cleanup, deduplication, consolidation)
Technology	IIS	• Regular system maintenance and testing • Training providers—providing training or pointing to sources (like CDC information) • "Think critically and use your clinical knowledge" • Be aware of alternative CDS services • Regular updates of the EHR with evaluated history with "as is" date • Capacity of the infrastructure
Technology	CDS functionality (internal or stand-alone)	• Regular system maintenance and testing • Training providers—providing training or pointing to sources (like CDC information) • "Think critically and use your clinical knowledge" • Be aware of alternative CDS services • Regular updates of the EHR with evaluated history with "as is" date • Capacity of the infrastructure

APPENDIX P EXAMPLE LIST OF BUSINESS CONTINUITY OPTIONS

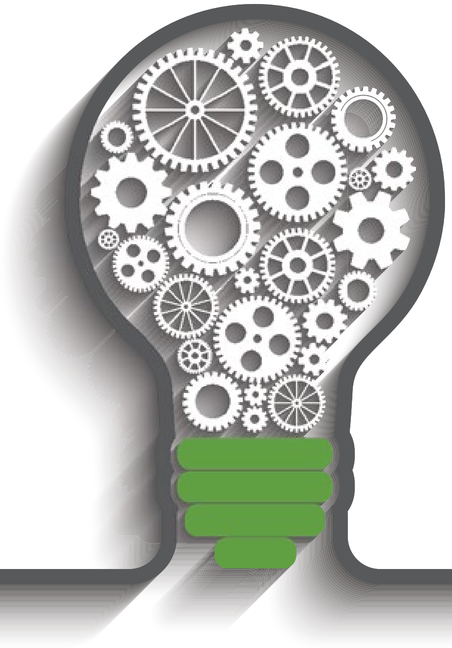
As described in Step 5.2 in Chapter 3, to identify business continuity options, consider measures that could help manage the disruption of a selected essential business function due to the loss of a resource.

There are several processes and tools that can guide the development of business continuity options. One tool is to work with a group of subject matter experts to develop a list of possible options. This appendix contains ideas brainstormed by the Business Continuity Workgroup for CDS for evaluation of patient immunization history (using EDE) when the IIS is the missing resource.

Continuity options for CDS for evaluation of patient immunization history (Using EDE) with IIS as the missing resource

Brainstormed options:

- Third-party service (e.g., Immunization Calculation Engine [ICE])—only in extreme situations
- Options—technology to run individual records
- Look for additional tools that could help with individuals or providers
- Maybe doctor/nurse on call who could help
- National Immunization Program (NIP) Info e-mail service—might be a longer process
- Direct providers to resources to help evaluate history
- EHRs may have CDS functionality
- See if the vendor can stand up a "copy" of the IIS



APPENDIX Q EXAMPLE USE CASES WITH BUSINESS CONTINUITY OPTIONS

> As described in Step 5.2 in Chapter 3, to identify business continuity options, consider measures that could help manage the disruption of a selected essential business function due to the loss of a resource.

There are several processes and tools that can guide the development of business continuity options. One tool that can be used is to apply a business continuity option to the normal operations use case for the selected essential business function to help determine how the option could work. The initial use cases were developed in Step 3.4 in Chapter 3, and examples are in Appendix J. This appendix contains examples of applying a business continuity option to the use cases for the three examples of selected essential business functions. As in Appendix J, this appendix combines the example selected essential business functions of access to demographic information and immunization history and CDS for evaluation of patient immunization history.

Continuity options for vaccine ordering capability

Missing resource: IIS; Continuity option: using paper process for ordering (alternative process)

	PROCESS STEP	NORMAL ("SUNNY DAY") SCENARIO	CONTINUITY OPTION ACTIVITIES
1	Provider organization staff submits a vaccine order to the awardee vaccine program.	**Activities:** Provider organization logs into the IIS via direct UI. Provider organization accesses ordering screen(s). Provider organization enters ordering information (orders, provider inventory, provider master data). Provider organization also enters additional information required by the vaccine program (e.g., information about temperature excursions in the storage units). Provider organization verifies the information is correct (e.g., delivery hours and contact information).	• Hold orders during the first couple of days. Then IIS program authorizes the use of a paper-based process. Consider ways to capture the input of information electronically. • IIS program has preexisting paper forms to capture the vaccine order and ending inventory information. • The vaccine ordering staff shares forms and instructions with each provider organization via one or more of the following methods: emailed via listserv, fax, posting on website. • The provider organization approval signature is captured. • The provider organization provides completed vaccine order and ending inventory forms to the IIS ordering staff via electronic survey tool, email, fax, or mail.

	PROCESS STEP	NORMAL ("SUNNY DAY") SCENARIO	CONTINUITY OPTION ACTIVITIES
2	Awardee vaccine program ordering staff approves the vaccine order.	**Activities:** Ordering staff logs into the IIS via direct UI. Ordering staff reviews additional information required by the vaccine program prior to approving the order. Ordering staff reviews, edits, and approves the order.	• Ordering staff reviews the order information and edits, if necessary. • Ordering staff reviews vaccine order and ending inventory submitted for the vaccine order. • Ordering staff approves or rejects the order.
3	Awardee vaccine program ordering staff submits the vaccine order to VTrckS.	**Activities:** Ordering staff exports the three files from the IIS into a desktop folder. Ordering staff logs into VTrckS and uploads files to VTrckS.	• Ordering staff logs into VTrckS. • Ordering staff obtains provider profile information from VTrckS or via the paper ordering process. • Ordering staff manually enters the information into VTrckS that is normally uploaded from the orders file, the provider inventory, and the provider master data. Alternatively, ordering staff creates a file that can be uploaded to VTrckS.
4	VTrckS validates and accepts the order.	**Activities:** VTrckS conducts internal checks.	• Continuity option is the same as normal operations.
5	Awardee vaccine program ordering staff gets information about the vaccine order fulfillment (shipment(s)). Use case ends.	**Activities:** Ordering staff logs into VTrckS to download the shipment information for the vaccine order and uploads into the IIS. This is a daily activity, with no notification.	• Ordering staff logs into VTrckS to download the shipment information for the vaccine order. • Ordering staff uses the file to check orders and saves file for possible future upload into IIS during the resumption phase. • Ordering staff may notify the provider of shipment information via mail merge or some other automated option.

Continuity option for access to demographic information and immunization history and CDS for evaluation of patient immunization history with resources – EDE

Missing resource: IIS; continuity option: using manual process (alternative process)

	PROCESS STEP	NORMAL ("SUNNY DAY") SCENARIO	CONTINUITY OPTION ACTIVITIES
1	Provider organization assembles patient identifying information.	**Activities:** Provider organization, using an EHR system, constructs an appropriately formatted and populated query that contains the patient's identifying information and provider organization information.	• Provider gathers patient information using EHR or patient chart.
2	Provider organization submits request for patient's demographic and immunization information to the IIS.	**Activities:** Provider organization, using an EHR, submits a query to an IIS as an electronic message for patient demographic information and patient immunization history.	• IIS staff informs provider that the system is down. • Provider calls IIS program or help desk. • IIS staff triages phone calls and help desk inquiries. • Priority is placed on providers calling while a patient is in the office. Priority may also depend on the type and size of the provider and circumstances (e.g., back-to-school clinic, outbreak). • EHR may still be sending queries that are in queue until disruption is resolved.
3	IIS assembles response information consisting of patient demographic information and patient immunization history.	**Activities:** IIS constructs an appropriately formatted and populated response that contains patient demographic information and patient immunization history.	• IIS staff uses information available, such as EHR, patient chart, clinical judgment, or other tools. • If database is available, develop process for looking up patient history on back end. • If database is also unavailable, data mart may be used for information.
4	IIS evaluates patient's immunization history and augments response information with evaluation results (valid/invalid doses).	**Activities:** IIS evaluates patient immunization history portion of the response and augments it with valid/invalid designation for vaccine doses.	• IIS staff evaluates record. This may be done by using an external web service or app to evaluate history and designate doses as valid/invalid.

	PROCESS STEP	NORMAL ("SUNNY DAY") SCENARIO	CONTINUITY OPTION ACTIVITIES
5	IIS evaluates patient immunization history portion of the response and augments it with recommended vaccine doses.	**Activities:** IIS evaluates patient immunization history portion of the response and augments it with recommended vaccine doses.	• IIS staff evaluates record. This may be done by using an external web service or app to evaluate history and recommend vaccine doses.
6	IIS submits response information to the provider organization.	**Activities:** IIS submits response (as an electronic message) to provider organization.	• Information is sent back to provider using secure means (e.g., phone, fax, secure email).
7	Provider organization receives and utilizes response from IIS. Use case ends.	**Activities:** Provider organization, using the EHR, receives and utilizes response (electronic message) from IIS.	• Provider receives information from IIS through secure means. Provider staff manually enters the information into its EHR. Provider utilizes the EHR in the same manner as normal operations.

Note: Continuity options for the CDS business function using direct UI are not included in this appendix. A workaround option of using a third-party service for CDS was identified but would completely circumvent the normal process, as the IIS would not be involved.

APPENDIX R EXAMPLE BUSINESS CONTINUITY OPTION TIMELINE

> As described in Step 5.2 in Chapter 3, to identify business continuity options, consider measures that could help manage the disruption of a selected essential business function due to the loss of a resource.

There are several processes and tools that can guide the development of business continuity options. One tool that can be used is a timeline developed to help visualize the timing of activities to implement the continuity option. This appendix contains examples of timelines to implement business continuity options for vaccine ordering capability and access to demographic information and immunization history.

Business Function: Providing vaccine ordering capability
Continuity Option: Using paper process for ordering

	0–24HRS	24HRS–1 WEEK	1 WEEK–1 MONTH	>1 MONTH
Internal Communications	Internal email to inform affected staff, next steps to resolve issue	Internal email to update staff on the issue, what is being done to resolve the issue, alternative process for external users	Internal email to update staff on the issue, what is being done to resolve the issue, alternative process for external users	Internal email to update staff on the issue, what is being done to resolve the issue, alternative process for external users, steps being taken to examine alternate processes for sustainability
External Communications	N/A	Targeted message to users that there is a delay in processing orders; if urgent need for vaccine, contact vaccine ordering staff	Targeted message to users on workaround process for ordering vaccine; include how to access paper form or online tool to submit orders	Targeted message to users with update on situation and workaround process for ordering vaccine
Alternative Process	N/A	Authorize use of paper form workaround process; get process in place to accept vaccine order information from providers and get information into VTrckS	Use paper forms or online data collection tool to receive vaccine orders; see use case with business continuity option	Use paper forms or online data collection tool to receive vaccine orders; see use case with business continuity option
Relocate	N/A	N/A	N/A	Examine other methods of providing vaccine ordering capability, including relocating to another IIS or direct user entry into VTrckS

Business Function: Access to demographic information and immunization history
Continuity Option: Manual workaround process

	0–24HRS	24HRS–1 WEEK	1 WEEK–1 MONTH	>1 MONTH
Internal Communications	Internal email to inform affected staff, next steps to resolve issue	Internal email to update staff on the issue, what is being done to resolve the issue, alternative process for external users	Internal email to update staff on the issue, what is being done to resolve the issue, alternative process for external users	Internal email to update staff on the issue, what is being done to resolve the issue, alternative process for external users
External Communications	Targeted message to users about issue, including steps being taken to resolve it, whom to contact with questions, and that program will communicate when issue is resolved	Targeted message to users about issue, alternative process for clinical decision support, and whom to contact with questions	Targeted message to users about issue, alternative process for clinical decision support, and whom to contact with questions	Targeted message to users about issue, alternative process for clinical decision support, and whom to contact with questions
Alternative Process	N/A	IIS staff uses resources available to evaluate patient history; see use case with business continuity option	IIS staff continues to use resources available to evaluate patient history, including external CDS service; see use case with business continuity option	IIS staff uses resources available to evaluate patient history, including external CDS service; additional staff may be brought on to support alternative process for longer period of time; see use case with business continuity option
Relocate	N/A	N/A	N/A	Examine other methods of providing clinical decision support, including relocating to another IIS

APPENDIX S EXAMPLE QUESTIONS FOR DETERMINING RESUMPTION OPTIONS

As described in Step 5.4 in Chapter 3, use the selected essential business functions and high-risk resources to practice resumption planning.

Resumption considerations assist with the process of restarting normal operations after a disruption has ended. It can be difficult to do significant preplanning for resumption since it is often highly dependent on the specifics of the disruption (e.g., length of time, business continuity options performed). However, practicing the process of developing resumption considerations can help determine broad concepts or questions to consider when restarting normal operations. This appendix contains examples of questions that can be helpful during resumption.

Was a manual alternative process utilized?

- Is data entry required to get the data into an electronic format?
- Could temporary staff be employed to help address any backlog?
- How will you confirm that all manual forms have been captured electronically?

How long was the continuity option employed? This may impact the extent of the resumption activity needed.

- Is it a staged resumption or all at once?
- Is there a massive data load required?
- Are there parallel processes required for a period of time during the resumption?

APPENDIX T COMMUNICATIONS – MESSAGE EXAMPLES

When a disruption occurs, communication with users is a critical component of a response.

Chapter 4.3 outlines key components of messaging, including initial messaging about the disruption and close-out messaging once functionality is restored. Any action steps on the part of the user should be clearly communicated in these messages. Below are example messages that can be modified to fit the specific conditions of a disruption.

EXAMPLE GENERIC INITIAL MESSAGE

Subject: Disruption to [FUNCTIONALITY]

It has come to our attention that [ISSUE – IIS is down, vaccine ordering function is unavailable, etc.].

We are working quickly to resolve this issue and apologize for any inconvenience this may cause. In the meantime, we ask that you [ACTION ITEM(S)]. Please contact the Help Desk with any urgent needs or questions at [EMAIL ADDRESS, PHONE].

We will let you know when [FUNCTION] is once again available. Thank you for your patience.

EXAMPLE GENERIC CLOSE-OUT MESSAGE

Subject: [FUNCTIONALITY] Has Been Restored

Thank you for your continued patience and understanding as we have worked through the technical issues with [IIS FUNCTION] over [TIME PERIOD]. This functionality has now been restored and is available for normal use.

What does this mean for you?
[ACTION STEPS FOR USERS]
Again, we thank you for your patience. We value your continued partnership in protecting [STATE] residents from vaccine-preventable diseases.

EXAMPLES OF MESSAGES TO ADDRESS SPECIFIC FUNCTIONALITY ISSUES

IIS unexpectedly down

Audience: Internal staff, external partners, IIS users

Message:

[IIS] is unexpectedly down. We are working to resolve the situation as quickly as possible. We will communicate again when we have more information.

We apologize for any trouble this downtime may cause you or your organization. Please contact the Help Desk at [EMAIL ADDRESS, PHONE] with any questions or concerns.

IIS back up from unexpected outage

Audience: Internal staff, external partners, IIS users

Message:

[IIS] was unexpectedly down from [TIME] to [TIME]. **[IIS] is now available for normal use.** If you **manually entered data** into the IIS web application anytime between [TIME, DATE] and [TIME, DATE], **your data were not saved and will need to be reentered.** We apologize for this inconvenience.

If your clinic reported **electronic data** to the IIS between these times, **you do not need to resend your data.** We will rerun the data we received during these times. Please note that there may be a delay in importing these data into [the IIS], as there is a backlog to process.

We apologize for any trouble this downtime may have caused you or your organization. Please contact the Help Desk at [EMAIL ADDRESS, PHONE] with any questions or concerns.

Vaccine ordering down

Audience: Internal staff, VFC ordering users

Message:

[IIS] vaccine ordering functionality is unexpectedly down. We are working to resolve the situation as quickly as possible. We will communicate again when we have more information. If you have recently placed an order, please be prepared to receive it at any time. The shipment information in the IIS and the shipment confirmation email may not reflect accurate shipment dates.

We apologize for any trouble this downtime may cause you or your organization. Please contact the Help Desk at [EMAIL ADDRESS, PHONE] with any questions or concerns.

Vaccine ordering back up

Audience: Internal staff, VFC ordering users

Message:

[IIS] vaccine ordering functionality is now available for normal use. There may be slight delays in processing orders as we work to fulfill a backlog of orders.

We apologize for any trouble this downtime may have caused you or your organization. Please contact the Help Desk at [EMAIL ADDRESS, PHONE] with any questions or concerns.

Data exchange down

Audience: Internal staff, regional coordinators, IT messaging team, data exchange users

Message:

[IIS] data exchange is unexpectedly down. We are working to resolve the situation as quickly as possible. We will communicate again when we have more information.

We apologize for any trouble this downtime may cause you or your organization. Please contact the Help Desk at [EMAIL ADDRESS, PHONE] with any questions or concerns.

Data exchange back up

Audience: Internal staff, regional coordinators, IT messaging team, data exchange users

Message:

Data exchange was unexpectedly down from [TIME] to [TIME]. **Data exchange is now available for normal use.** If your organization attempted to send data during the downtime, please review your interface and ensure those data are resent.

We apologize for any trouble this downtime may have caused you or your organization. Please contact the Help Desk at [EMAIL ADDRESS, PHONE] with any questions or concerns.

Immunization history page down

Audience: Internal staff, regional coordinators, IIS users

Message:

The immunization history and forecasting page is currently unavailable through the [IIS] user interface. We are working to resolve this situation as quickly as possible. We will communicate again when we have more information.

We apologize for any trouble this downtime may cause you or your organization. Please contact the Help Desk at [EMAIL ADDRESS, PHONE] with any questions or concerns.

Immunization history page back up

Audience: Internal staff, regional coordinators, IIS users

Message:

The [IIS] immunization history and forecasting page through the user interface was unavailable from [TIME] to [TIME]. The page is now available for normal use.

We apologize for any trouble this downtime may have caused you or your organization. Please contact the Help Desk at [EMAIL ADDRESS, PHONE] with any questions or concerns.

Reports issue

Audience: Internal staff, RCs, specific report users

Message:

Reports in [IIS] are currently [PROBLEM(S)]. We are working to resolve this issue as quickly as possible. Until it is resolved, [users will not be able to access reports/reports will not have accurate data]. We will communicate again when the issue is resolved.

We apologize for any trouble this issue may cause you or your organization. Please contact the Help Desk at [EMAIL ADDRESS, PHONE] with any questions or concerns.

Reports restored

Audience: Internal staff, regional coordinators, specific report users

Message:

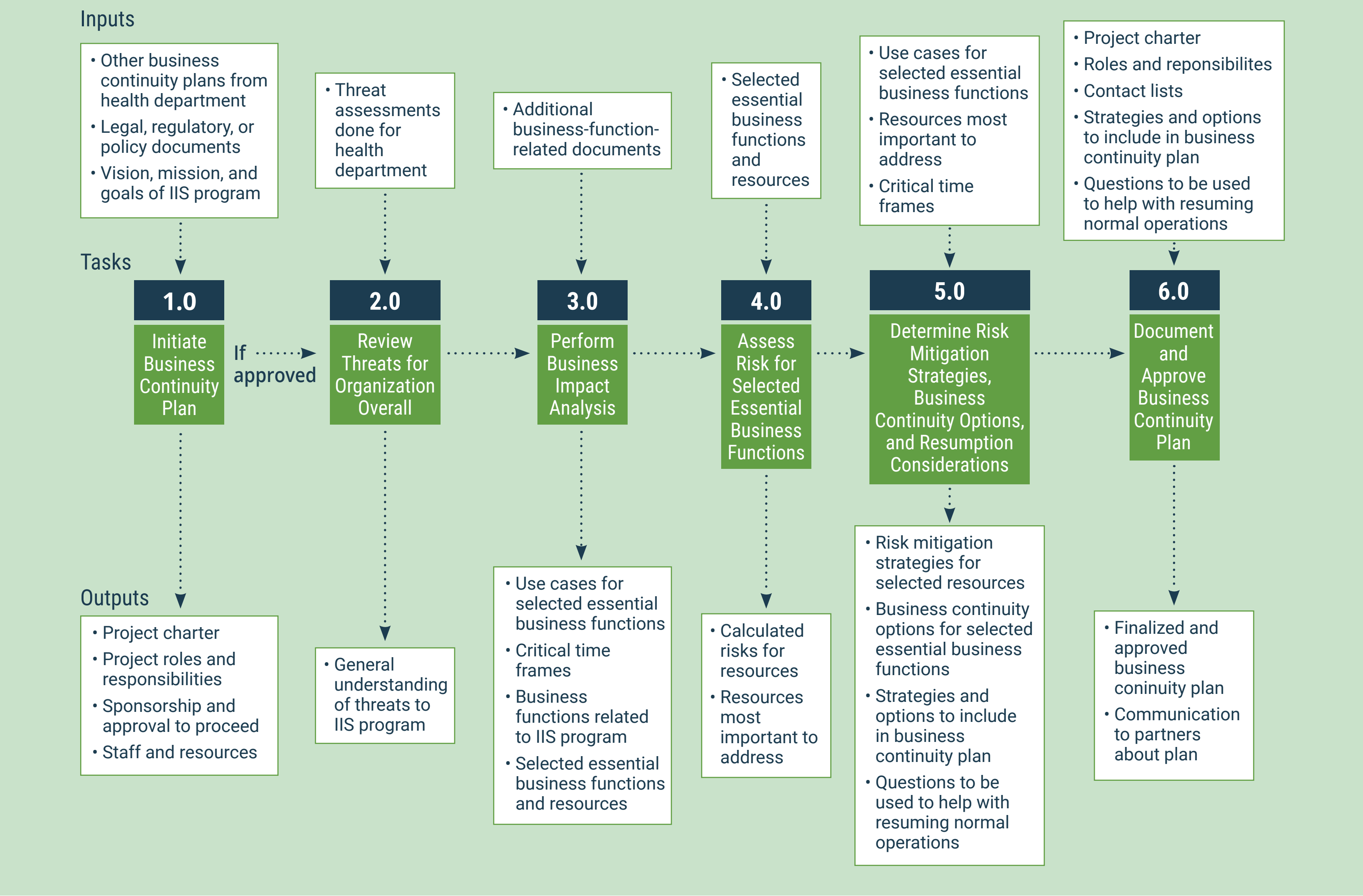
[IIS] reports were [PROBLEM(S)] from [TIME] to [TIME]. They are now available for normal use.

We apologize for any trouble this issue may have caused you or your organization. Please contact the Help Desk at [EMAIL ADDRESS, PHONE] with any questions or concerns.

APPENDIX U TASK INPUT AND OUTPUT DIAGRAM

The following diagram lists the inputs and outputs for each high-level task in the business continuity planning process.

Figure 8 | *Task input and output diagram*



Inputs

- Other business continuity plans from health department
- Legal, regulatory, or policy documents
- Vision, mission, and goals of IIS program

- Threat assessments done for health department

- Additional business-function-related documents

- Selected essential business functions and resources

- Use cases for selected essential business functions
- Resources most important to address
- Critical time frames

- Project charter
- Roles and reponsibilites
- Contact lists
- Strategies and options to include in business continuity plan
- Questions to be used to help with resuming normal operations

Tasks

1.0 Initiate Business Continuity Plan

If approved

2.0 Review Threats for Organization Overall

3.0 Perform Business Impact Analysis

4.0 Assess Risk for Selected Essential Business Functions

5.0 Determine Risk Mitigation Strategies, Business Continuity Options, and Resumption Considerations

6.0 Document and Approve Business Continuity Plan

Outputs

- Project charter
- Project roles and responsibilities
- Sponsorship and approval to proceed
- Staff and resources

- General understanding of threats to IIS program

- Use cases for selected essential business functions
- Critical time frames
- Business functions related to IIS program
- Selected essential business functions and resources

- Calculated risks for resources
- Resources most important to address

- Risk mitigation strategies for selected resources
- Business continuity options for selected essential business functions
- Strategies and options to include in business continuity plan
- Questions to be used to help with resuming normal operations

- Finalized and approved business coninuity plan
- Communication to partners about plan

APPENDIX V ACKNOWLEDGEMENTS

AIRA would like to acknowledge and thank the following individuals and organizations for their support and assistance:

- Individual subject matter experts who contributed their expertise through telephone interviews:
    - Valentin Shoshtarikj, Arizona
    - Heather Roth, Colorado
    - Patricia Swartz, Maryland
    - Aaron Bieringer, Minnesota
    - Miriam Muscoplat, Minnesota
    - Amanda (Mandy) Harris, Nevada
    - Mary Woinarowicz, North Dakota
    - Jenne McKibben, Oregon
    - Mike Day, Oregon
    - Lee Peters, Oregon
    - Ivan Garcia, Puerto Rico
    - Norma Castro, Puerto Rico
    - Veronica Rodriguez, Puerto Rico
    - Dannette Dronenburg, Washington
    - Karen Meranda, Washington
    - Michele Roberts, Washington
    - Katie Reed, DXC
    - Gary Wheeler, DXC
    - Claire Murchie, Envision Technology Partners
    - Steve Murchie, Envision Technology Partners
    - Brandy Altstadter, Scientific Technologies Corporation
    - Ashley McDonald, Scientific Technologies Corporation
- Individual subject matter experts who contributed their expertise in the Business Continuity Workgroup through facilitated in-person discussion and document review:
    - Valentin Shoshtarikj, Arizona
    - Heather Roth, Colorado
    - David McCormick, Indiana
    - Amy Metroka, New York City
    - Miriam Muscoplat, Minnesota
    - Amanda (Mandy) Harris, Nevada
    - Mary Woinarowicz, North Dakota
    - Lee Peters, Oregon
    - Dannette Dronenburg, Washington
    - Jan Hicks-Thomson, CDC

- The MIROW Steering Committee, which selected the topic of business continuity, provided input at various stages of the effort and reviewed and provided comment on the final guide:
    - Baskar Krishnamoorthy, Florida
    - David McCormick, Indiana
    - Miriam Muscoplat, Minnesota
    - Amanda (Mandy) Harris, Nevada
    - Megan Meldrum, New York
    - Amy Metroka, New York City
    - Katie Reed, DXC
    - Brandy Altstadter, Scientific Technologies Corporation
    - Elaine Lowery, AIRA
    - David Lyalin, CDC
    - Warren Williams, CDC
- The AIRA board of directors, who provided input at various stages of the effort and/or reviewed and provided comment on the final guide:
    - *President* • Amanda (Mandy) Harris, Nevada
    - *President-Elect* • Aaron Bieringer, Minnesota
    - *Immediate Past President* • Kim Salisbury-Keith, Rhode Island
    - *Secretary* • Jenne McKibben, Oregon
    - *Treasurer* • Heather Roth, Colorado
    - *Member-at-Large* • David McCormick, Indiana
    - *Directors*
        - Bridget Ahrens, Vermont Immunization Registry
        - Dannette Dronenburg, Washington
        - Christy Gray, Virginia
        - Nathalie Hartert, Tennessee
        - Jeffrey McIntyre, Mississippi
        - Kevin Dombkowski, University of Michigan, Child Health Evaluation and Research Unit
        - Steve Murchie, Envision Technology Partners
- The AIRA staff and consultants who contributed to this document's development:
    - Rebecca Coyle, AIRA Executive Director
    - Alison Chi, AIRA Policy and Planning Director
    - Beth Parilla, AIRA Senior Program Manager*
    - Nichole Lambrecht, AIRA Senior Project Manager*
    - Elaine Lowery, AIRA Consultant*
    - Elizabeth Langford, AIRA Consultant*
    - Tom Bang-Knudsen, AIRA Consultant (Business Continuity Subject Matter Expert)
    - Jim Pearsol, Facilitator

*MIROW Small Group Members

- The CDC staff and consultants who contributed to this document's development:
  - David Lyalin, CDC*
  - Cindy Scullion, Business Rules Solutions*

- Independent copy editors who reviewed and edited the guide
  - Ginger Redmon, Writer/editor with CDC
  - Maureen Brody, Copy/editing services contracted through AIRA

- Individuals, in addition to the subject matter experts, who provided feedback during the review process:
  - Brandy Altstadter, Scientific Technologies Corporation
  - Cherie Thomas, Trey Industries, Inc.
  - Eric Larson, AIRA
  - Janet Fath, CDC
  - Noam Arzt, HLN Consulting, LLC
  - Patricia Swartz, Maryland
  - Steve Murchie, Envision Technology Partners
  - Sharon Polek, Michigan
  - Susan Salkowitz, Salkowitz Associates, LLC
  - Tammy LeBeau, South Dakota
  - Veronica Rodriguez, Puerto Rico

*MIROW Small Group Members