3 Types of Continuity Plans
Why They are Needed
How to Get Started

6 April 2021

Gregory B. White, Ph.D.
CIAS-ISAO
The Center for Infrastructure Assurance and Security
The University of Texas at San Antonio

CIAS-ISAO
COMMUNITY CYBERSECURITY PROGRAMS

The CIAS at UTSA

The Center for Infrastructure Assurance and Security

- Established in 2001 at The University of Texas at San Antonio
- Operationally focused – How can we improve cybersecurity **today**!
- Leading the advancement of state, local, tribal and territorial (SLTT) cybersecurity capabilities and collaboration.

The CIAS Today

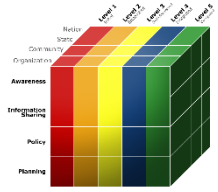
SLTT and Training

Running Exercises Since 2002

CIAS-ISAO
COMMUNITY CYBERSECURITY PROGRAMS

(ISC)²

UDLAP
UNIVERSIDAD DE LAS AMERICAS PUEBLA



TEXAS ISAO

ISAO
Standards Organization

FEMA

Competitions

Hosting Competitions Since 2005

PANOPLY

CCDC
NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION

HIVESTORM

eSentinel

Culture of Cybersecurity & Gaming

Supporting K-12 Education

Research

Conducting Research for 20 Years

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

U.S. DEPARTMENT OF HOMELAND SECURITY

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

CIAS-ISAO Continuity Planning Webinar
April 6, 2021

Cyber Continuity Planning

- Why is it needed?
- What is it?
- Variety of Plans
- Where can you start?
- Resources

Continuity Planning: **Why is it Needed?**

- There are many different events that can cause an interruption in the operation of your organization.
  - Natural Disasters, Manmade Disaster, Cyber Attacks
- Interruptions due to cyber events are becoming increasingly common.
  - Breaches, Ransomware, Insiders, Misconfigurations, SW errors
- How long can your organization last without Mission Essential Functions (MEF)?

Continuity Planning
Why is it Needed? Some Examples

Cybersecurity and your water: Hacker attempted to poison Florida city's water supply

THE HILL 02/23/21 11:30 AM EST

1,852 Cyber Attacks Hit India Each Minute Last Year; Mumbai, Delhi Most Affected

According to the Quick Heal Annual Threat Report 2019, the metropolitans of Mumbai, Delhi, Bengaluru and Kolkata are the most attacked cities in India, in terms of online attacks.

News18.com | Updated:September 3, 2019, 10:57 PM IST

Baltimore estimates cost of ransomware attack at $18.2 million as government begins to restore email accounts

By IAN DUNCAN
THE BALTIMORE SUN | MAY 29, 2019 | 7:45 PM

The damage from Atlanta's huge cyberattack is even worse than the city first thought

Taylor Hatmaker @tayhatmaker / 1 year ago

TECH

Alarm in Texas as 23 towns hit by 'coordinated' ransomware attack

PUBLISHED MON, AUG 19 2019 • 9:58 AM EDT | UPDATED 4 HOURS AGO

Louisiana's governor declares an emergency after cyberattacks on several school systems

Hong Kong Cyber Attack Briefly Disrupts Key Protester Forum

By Shelly Banjo
August 30, 2019, 11:53 PM CDT

Crippling ransomware attacks targeting US cities on the rise

By Kevin Collier, CNN
Updated 10:34 PM ET, Fri May 10, 2019

Albany, NY, is coping with a ransomware attack

By Kevin Collier, CNN
Updated 8:19 AM ET, Sat April 6, 2019

KC suburb spent millions on cyber security protections but still got hit by ransomware

BY KEVIN HARDY
DECEMBER 12, 2020 05:00 AM

OnlineAthens
ATHENS BANNER-HERALD

Cyber attack forces Jackson County to pay $400K ransom

By Wayne Ford
Posted Mar 8, 2019 at 3:13 PM
Updated Mar 8, 2019 at 3:13 PM

(Georgia)

Hit by Ransomware Attack, Florida City Agrees to Pay Hackers $600,000

23 AUG 2019 NEWS
City of London Hit by One Million Cyber-Attacks Per Month

CIAS-ISA
COMMUNITY CYBERSECURITY PROGRAMS

UTSA

Continuity Planning: **What is it?**

- The purpose of *Contingency Planning* is to prepare for the possibility of an interruption in your organization's operations.
  - We will focus on Cyber Continuity Planning
- For Example: A Continuity of Operations (COOP) Plan
  - "Provides procedures and guidance to sustain an organization's mission essential functions (MEFs) at an alternate site for up to 30 days; mandated by federal directives." (from NIST SP 800-34 Rev. 1)
- There are several different types of documents, each focused on a specific aspect of contingency (continuity) planning.

Continuity Planning: **A Variety of Plans**

- Continuity of Operations **(COOP)**
  Provides procedures and guidance to sustain an organization's mission essential functions (MEFs) at an alternate site for up to 30 days
- Business Continuity Plan **(BCP)**
  Mission/business process focused plan that may be activated in coordination with a COOP plan to sustain non-mission essential functions (MEFs).
- Information Systems Contingency Plans **(ISCP)**
  Provides procedures and capabilities for recovering an information system
- Disaster Recovery Plan **(DRP)**
  A DRP is an information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency.
- Business Impact Analysis **(BIA)**
  A systematic process to determine and evaluate the potential effects of an interruption to critical **business** operations as a result of a disaster, accident or emergency.

(from NIST SP 800-34 Rev. 1 and https://searchstorage.techtarget.com/definition/business-impact-analysis)

Continuity Planning:
Where Can You Start – Basics

- You need to identify your Mission Essential Functions. What does your organization need in order to sustain critical operations?
- What data and computers are needed to maintain your MEFs? What personnel?
- Especially for small organizations, don't get overwhelmed by the plethora of different plans

Let's Begin with a BIA

- Let's start by determining what the impact will be to your organization should a disruptive event occur.
- This will help determine what business operations are essential to continue with the organization's mission.
- Remember what we said a BIA is: "A systematic process to determine and evaluate the potential effects of an interruption to critical **business** operations as a result of a disaster, accident or emergency. "

Continuity Planning: **Parts of a BIA**

- So, what will be the impact to your organization should a disruptive event occur?
- Determining this will help you learn what business operations are essential to continue with your organization's mission.
- A BIA may include the following areas:
  - Technology
  - People
  - Process & Policy
  - Organization
  - Business Strategy
- We will focus on the technology (IT) portion of this.

Continuity Planning: **BIA Questions – Business Overview**

1. Business Unit Overview

Provide a brief description of your unit/division's functions.	
What are the unit's normal work hours? How many personnel currently work in the department?	
What is the average work volume (e.g. number of business registered, number of audits completed, number of timesheets entered, etc.) processed by the unit?	
Where applicable, relate work volume mentioned above to dollars or revenue. (Revenue going out, revenue retrieved from registration fees, etc.)	
Does the unit have a peak volume or other critical time frames? If yes, when are these periods? (e.g. Elections happen in November, payments processed at the end of the month, etc.)	

Continuity Planning: **BIA Questions – Key Processes**

2. Key Business Processes

Identify and describe the **key** business processes of the unit/division. For each process, identify its ***Recovery Time Objective (RTO)***. **RTO** is defined as how quickly the process must be restored following a disaster. The Recovery Time Objective is an estimate of how long the process can be unavailable. Also identify a ***Recovery Point Objective (RPO)*** for each process. **RPO** is the determination of how much data loss, in terms of time, is tolerable before a process is significantly impacted. If the process can be performed manually, please use Attachment A to explain. Use multiple pages if needed.

Key Business Process	Recovery Time Objective*	Recovery Point Objective**	Can this be performed manually? For how long? ***	Computer Systems/Applications required to perform this process

* *Recovery Time Objective in terms of hours, days, or weeks*
** *Recovery Point Objective in terms of hours, days, or weeks*
*** *If process can be performed manually, list manual processes in Attachment A*

CIAS-ISA
COMMUNITY CYBERSECURITY PROGRAMS

UTSA

Continuity Planning: **BIA Questions - Impact**

3. Quantitative & Qualitative Impact Estimates

For each process listed in "Section 2 - Key Business Processes," enter the process name on the next page and complete one page per item. First, quantify the estimated dollar loss incurred as a result of a disruption of the business process listed. Second, identify the intangible business interruption impacts incurred as a result of a disruption of the business process. Use the scoring numbers (0-4) provided in the legend below.

For the purposes of this questionnaire, assume it is midway through the budget cycle (June). *If the quantitative or qualitative impact will vary at different points in the biennium cycle, please use the "Comments" section to explain how and why the impact will change, as well as what will trigger the change.*

Examples:

- If a server system had to be replaced at the beginning of the biennium, it would have a lower impact than if it had to be replaced near the end of the biennium when funds are lower.
- A disruption to business processes in the Elections division would have catastrophic qualitative impacts on Election Day in November, but no to low impact most of the time.

QUANTITATIVE IMPACT ESTIMATES				
Scoring	**Low Range**		**High Range**	**Impact to Business or Operations**
0	0	<	$500,000	No to Low
1	$500,000	But <	$1,000,000	Low to Moderate
2	$1,000,000	But <	$3,000,000	Moderate
3	$3,000,000	But <	$6,000,000	Moderate to High
4	$6,000,000	And greater		High to Catastrophic

QUALITATIVE IMPACT ESTIMATES	
Scoring	**Impact to Business or Operations**
0	No to Low
1	Low to Moderate
2	Moderate
3	Moderate to High
4	High to Catastrophic

BIA Questions – Impact (cont.)

BUSINESS PROCESS NAME: _____

Category of Quantitative Loss	$ Impact 0 to 1 week	$ Impact 1 to 2 weeks	$ Impact 2 to 3 weeks	$ Impact 3 weeks to 1 month	$ Impact 1 month +
Loss of Current Business					
Loss of Future Business					
Increase in Operating Costs					
Increase in Interest Income Loss					
Non-Performance Penalties					
Delay in Billing or Payments					
Cash Flow Impact to Agency					
Potential Liability Cost					
Loss of Productivity					
Category of Qualitative Loss	**Impact 0 to 1 week**	**Impact 1 to 2 weeks**	**Impact 2 to 3 weeks**	**Impact 3 weeks to 1 month**	**Impact 1 month +**
Degraded Customer Service					
Degraded Public Confidence or Image					
Noncompliance with Government Regulations					
Noncompliance with Contracts and SLA's					
Degraded Quality of Work					
Loss of Stakeholder confidence					
Delay Delivery of Internal Products/Services					
Delay Delivery of External Products/Services					

Comments:

Continuity Planning: **BIA Questions – Regulatory Requirements**

4. Identification of Regulatory, Legal, or Service Level Requirements

Briefly describe any regulatory, legal, or customer service level requirements (e.g. ORS, OAR, Accreditation, State Licensing, etc.) associated with the business processes identified in "Section 2 - Business Processes" that would be impacted if a disruption interrupted business unit operations.

Key Business Process Impacted	Regulatory Requirement, Legal, Service Level Expectation, etc.

Continuity Planning: **BIA Questions – Inter-Dependencies**

5. Business unit Inter-dependencies (work received and work sent)

List any internal business units, in-house central computer systems, data processing service bureaus, or other external entities from which your department receives work and/or sends work to in performing its key business processes. Use multiple pages if needed. If a workflow has been documented for a business process, attach as Attachment B.

Business Process Receiving and Sending the Work	WORK INPUTS Type of Work/Data Received, Frequency Received	RECEIVED FROM Business Unit, Computer System, or Organization from which the Work is Received	WORK OUTPUT Type of Work/Data Sent, Frequency Sent	SENT TO Business Unit, Computer System, or Organization to which the Work is Sent
Example: "The Process" *Process contract requests*	What goes into it? How often? *Request for services, varies*	Who do you get it from? *SOS staff*	What do you do with it? How often? *Bid requests, final contracts, varies*	Who does it go to? *Service providers, contractors*

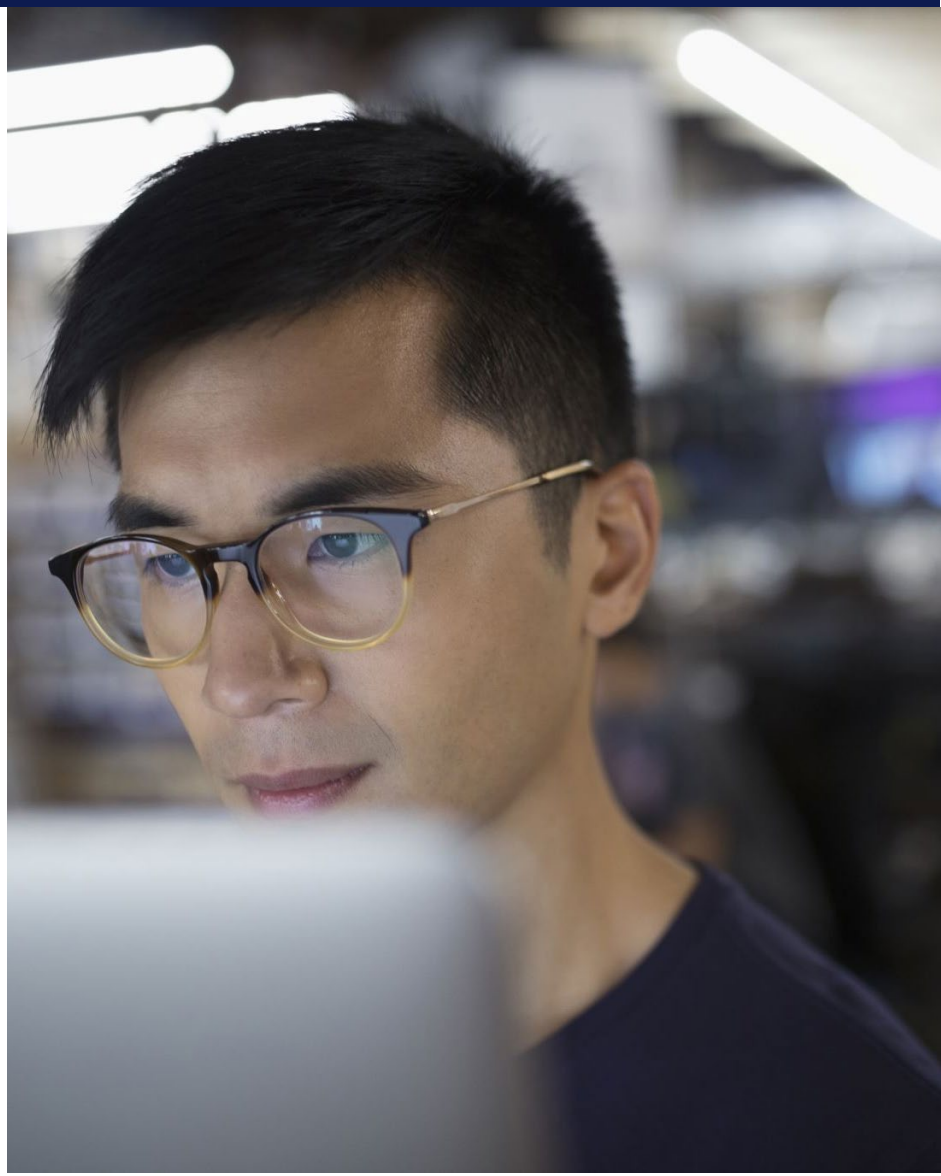
https://www.oregon.gov/das/Procurement/Guiddoc/BusImpAnalysQs.doc

Next, Let's Work on an ISCP

- When you went through your BIA you identified computers and applications your business functions required.

- Let's next take a look at an Information Systems Contingency Plan (ISCP)

- Remember, the ISCP provides procedures and capabilities for recovering an information system



Continuity Planning: **Parts of an ISCP**

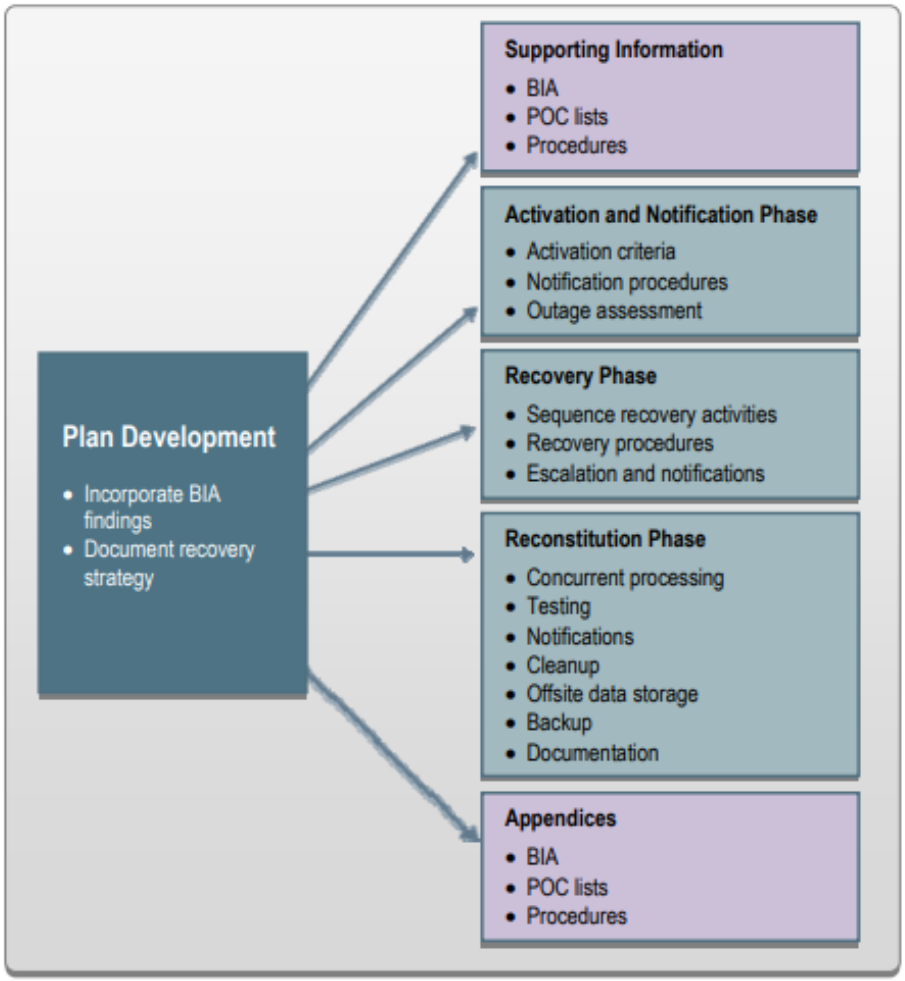


Figure 4-1: Contingency Plan Structure

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Parts of an ISCP - Introduction

Introduction Section

- Background. This subsection establishes the reason for developing the ISCP and defines the plan objectives.
- Scope. The scope identifies the FIPS 199 impact level and associated RTOs as well as the alternate site and data storage capabilities (as applicable).
- Assumptions. This section includes the list of assumptions that were used in developing the ISCP as well as a list of situations that are not applicable.
- System description. It is necessary to include a general description of the information system addressed by the contingency plan. The description should include the information system architecture, location(s) and any other important technical considerations.
- Overview of three phases. The ISCP recovery is implemented in three phases: (1) Activation and Notification, (2) Recovery and (3) Reconstitution.
- Roles and responsibilities. The roles and responsibilities section presents the overall structure of contingency teams, including the hierarchy and coordination mechanisms and requirements among the teams. The section also provides an overview of team member roles and responsibilities in a contingency situation. Teams and team members should be designated for specific response and recovery roles during contingency plan activation.

Parts of an ISCP - Activation

The Activation and Notification Phase defines initial actions taken once a system disruption has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the plan. At the completion of the Activation and Notification Phase, ISCP staff will be prepared to perform recovery measures to restore system functions.

- **Activation Criteria and Procedure**
  - The ISCP is activated if one or more of the activation criteria for that system are met.
    - Extent of any damage to the system (e.g., physical, operational, or cost);
    - Criticality of the system to the organization's mission; and
    - Expected duration of the outage lasting longer than the RTO.
- **Notification Procedures**
  - Describe how to notify recovery personnel during business and non-business hours.
- **Outage Assessment**
  - It is essential to assess the nature and extent of the disruption
    - Cause of the outage or disruption;
    - Potential for additional disruptions or damage;
    - Status of physical infrastructure (e.g., structural integrity of computer room, condition of power, telecommunications, and HVAC);
    - Inventory and status of equipment (e.g., fully-, partially-, or non-functional);
    - Type of damage to system equipment or data (e.g., water, fire, electrical surge);
    - Items to be replaced (e.g., hardware, software, supporting materials); and
    - Estimated time to restore normal services.

Parts of an ISCP - Recovery

- Formal recovery operations begin after the ISCP has been activated, outage assessments have been completed (if possible), personnel have been notified, and appropriate teams have been mobilized.
- Recovery Phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or new alternate location.
  - **Sequence of Recovery Activities**
    - Provide a stepwise, sequence so system components may be restored in a logical manner.
  - **Recovery Procedures**
    - Provide detailed procedures to restore the information system or components to a known state.
  - **Recovery Escalation and Notification**
    - Actions would include additional notifications for more recovery staff, messages and status updates to leadership, and notices for additional resources

Parts of an ISCP - Reconstitution

During Reconstitution, recovery activities are completed, and normal system operations are resumed. If the original facility is unrecoverable, activities in this phase can also be applied to preparing a new permanent location to support system processing requirements.

- **Validating Successful Recovery**
  - Concurrent Processing. Running a system at two locations concurrently until there is a level of assurance that the recovered system is operating correctly and securely.
  - Validation Data Testing. Testing and validating recovered data to ensure files & databases have been recovered completely and are current to the last backup.
  - Validation Functionality Testing. Verifying that all system functionality has been tested, and the system is ready to return to normal operations.
- **Deactivation of the Plan**
  - The process of returning the system to normal operations and finalizing reconstitution activities to prepare the system against another outage or disruption. These activities include notifications, cleanup, data storage and backup, and documentation.

Parts of an ISCP - Template

- NIST SP 800-34r1 has a template for an ISCP that can be followed:

  https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

- Remember that you will need an ISCP for each of the systems needed for your Mission Essential Functions.

Continuity Planning
Our Third Document – the COOP

The last document we will look at today is the COOP.

- Remember the purpose of a Continuity of Operations (COOP)
  - Provides procedures and guidance to sustain an organization's mission essential functions (MEFs) at an alternate site for up to 30 days
- This plan will be much more extensive as it is designed to address all of your MEFs and the systems needed by them.
- A COOP template can be found at
  - https://www.fema.gov/pdf/about/org/ncp/coop/continuity_plan_federal_d_a.pdf

Parts of a COOP - Scope

SCOPE

This section describes the applicability of the plan to the organization as a whole, headquarters as well as subordinate activities, co-located and geographically dispersed, and to specific personnel groups in the organization. It should also include the scope of the plan. Ideally, plans should address the full spectrum of potential threats, crises, and emergencies (natural and man-made). Sample text for this section includes:

- *This Plan applies to the functions, operations, and resources necessary to ensure the continuation of [Organization Name]'s essential functions, in the event its normal operations at [Name primary operating facility] are disrupted or threatened with disruption. This plan applies to all [Organization Name] personnel. [Organization Name] staff must be familiar with continuity policies and procedures and their respective continuity roles and responsibilities*

Parts of a COOP – Situation Overview

SITUATION OVERVIEW

The situation section characterizes the "planning environment," making it clear why a continuity of operations plan is necessary. In this section, organizations should reference their risk assessment to summarize the hazards faced by their organization and the relative probability and impact of the hazards. Sample text for this section includes:

- *The [Organization Name] continuity facilities were selected following an all-hazards risk assessment of facilities for continuity operations use. The [Organization Name] risk assessment is found at [insert document name and location or insert risk assessment information in this section of the plan]. This risk assessment addresses the following for each continuity facility:*
  - *Identification of all hazards*
  - *A vulnerability assessment to determine the effects of all hazards*
  - *A cost-benefit analysis of implementing risk mitigation, prevention, or control measures*
  - *A formal analysis by management of acceptable risk*
  - *…*

Parts of a COOP – Planning Assumptions

PLANNING ASSUMPTIONS

This section should briefly describe the layout of the continuity of operations plan and familiarize the readers with underlying assumptions made during the planning process. Sample text for this section includes:

- ***This Continuity Plan is based on the following assumptions:***
  - *An emergency condition may require the relocation of [Organization Name]'s Emergency Relocation Group (ERG) members to the continuity facility at [continuity facility name]*
  - *The [continuity facility name] will support ERG members and the continuation of [Organization Name] essential functions by available communications and information systems within 12 hours or less from the time the Continuity of Operations Plan is activated, for potentially up to a 30-day period or until normal operations can be resumed*
  - *[Organization Name] regional operations are unaffected and available to support actions directed by the [title of organization head] or his successor. However, in the event that ERG deployment is not feasible due to the loss of personnel, the [Organization Name] will devolve to [list devolution office/region]*
  - *[Insert additional assumptions here]*

Parts of a COOP – Objectives

OBJECTIVES

All plans and procedures should list the objectives that the plans are designed to meet. Continuity planning objectives are pre-identified in Federal Continuity Directive 1. Sample text for this section includes:

- ***The [Organization Name] continuity objectives are listed below:***
  - *(1) Ensure that [Organization Name] can perform its Mission Essential Functions (MEFs) and Primary Mission Essential Functions (PMEFs), if applicable, under all conditions*
  - *(2) Reduce the loss of life and minimize property damage and loss*
  - *(3) Execute a successful order of succession with accompanying authorities in the event a disruption renders [Organization Name] leadership unable, unavailable, or incapable of assuming and performing their authorities and responsibilities of the office*
  - *(4) Reduce or mitigate disruptions to operations*
  - *(5) Ensure that [Organization Name] has facilities where it can continue to perform its MEFs and PMEFs, as appropriate, during a continuity event*
  - *(6) Protect essential facilities, equipment, records, and other assets, in the event of a disruption*
  - *(7) Achieve [Organization Name]'s timely and orderly recovery and reconstitution from an emergency*
  - *(8) Ensure and validate continuity readiness through a dynamic and integrated*

Parts of a COOP – Security & Privacy

SECURITY AND PRIVACY STATEMENT

This section details the classification of the Continuity Plan. At a minimum, agencies should classify their plan as "For Official Use Only," as continuity plans and procedures are sensitive, organization-specific documents. Further, if your continuity plan includes a roster of continuity personnel that includes personal information, such as telephone numbers, that information is protected under the Privacy Act of 1974. Organizations should consult with their Office of Security, or similar office, to ensure their continuity plans and procedures are properly classified and marked. This section should also contain dissemination instructions, including to whom and via what means the agency will disseminate the plan. **Sample text for this section includes:**

- *[Organization Name, office name] will distribute copies of the Continuity Plan on a need to know basis. [Insert procedures for distributing the plan to ERG members and all personnel, e.g. via hard or electronic copy or posting on internal websites]. In addition, copies of the plan will be distributed to other organizations as necessary to promote information sharing and facilitate a coordinated interagency continuity effort. Further distribution of the plan, in hardcopy or electronic form, is not allowed without approval from [insert office or position title]. [Organization Name, office name] will distribute updated versions of the Continuity Plan annually or as critical changes occur.*

Parts of a COOP – Concept of Operations

CONCEPT OF OPERATIONS

This section will explain how the organization will implement its Continuity of Operations Plan, and specifically, how it plans to address each critical continuity of operations element. This section should be separated into four phases: readiness and preparedness, activation and relocation, continuity facility operations, and reconstitution. Devolution planning strongly correlates in each phase, and is also addressed in this section.

COOP Concept of Operations

- Phase 1: Readiness and Preparedness
  - Readiness is the ability of an organization to respond to a Continuity event. This phase includes all agency Continuity Readiness and Preparedness activities.
- Phase 2: Activation and Relocation
  - This phase should explain Continuity of Operations Plan activation procedures and relocation procedures from the primary facility to the Continuity facility. The Plan must provide a process or methodology for attaining operational capability at the Continuity site(s) with minimal disruption to operations within 12 hours of Plan activation. This section should also address procedures and guidance for non-relocating personnel.
- Phase 3: Continuity Operations
  - This phase identifies initial arrival procedures as well as operational procedures for the continuation of Essential Functions.
- Phase 4: Reconstitution Operations
  - Organizations must identify and outline a plan to return to normal operations once organization heads or their successors determine Reconstitution operations for resuming normal business operations can be initiated.

From: Continuity of Operations Plan Template for Federal Departments and Agencies
https://www.fema.gov/sites/default/files/2020-07/COOP-Planning-Template_091813.pdf

Parts of a COOP – Devolution

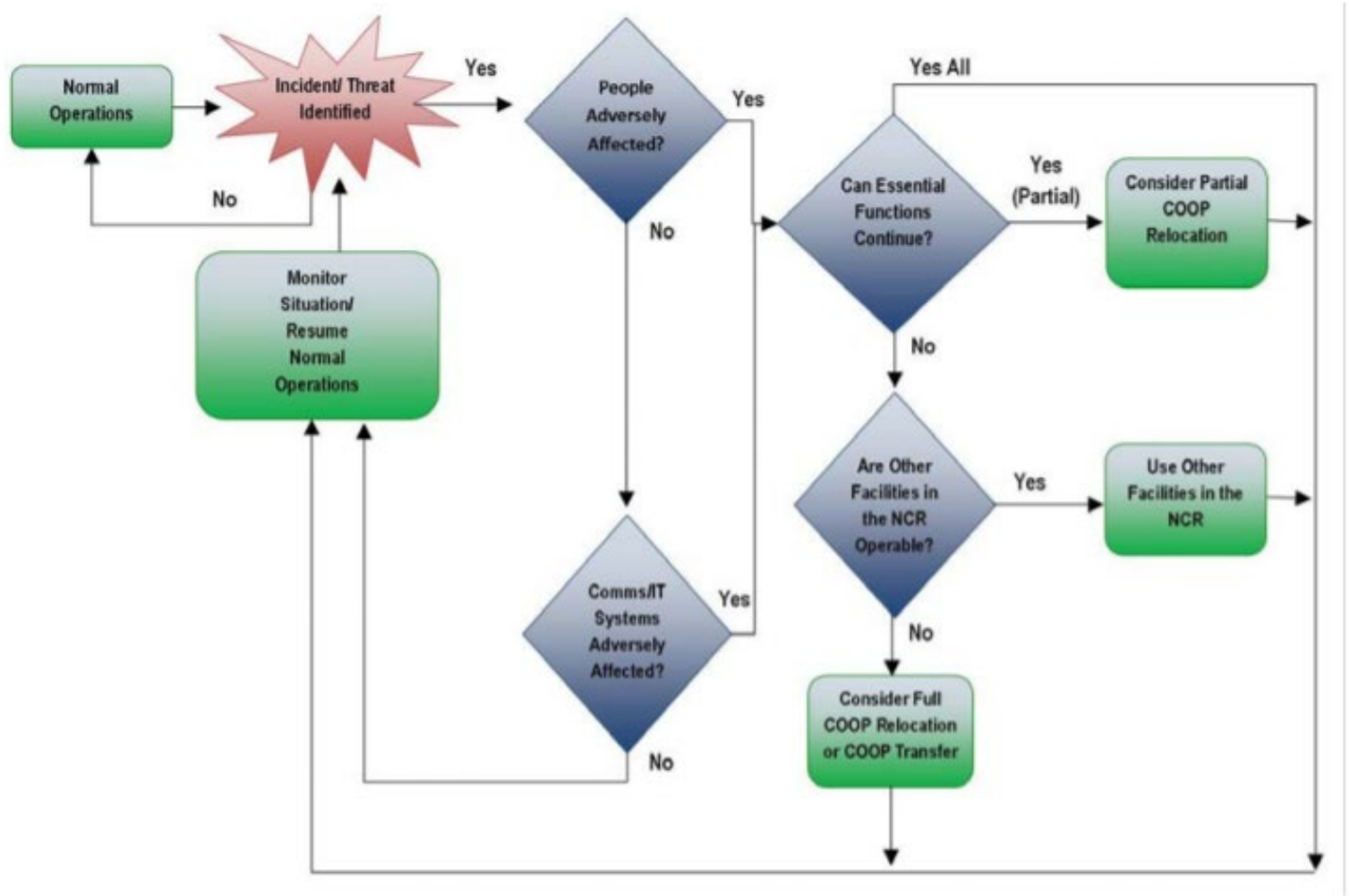
DEVOLUTION OF CONTROL AND DIRECTION

Devolution planning supports overall continuity planning and addresses the full spectrum of threats and all-hazards emergency events that may render an organization's leadership or staff unavailable to support, or incapable of supporting, the execution of the organization's essential functions from either its primary location or its continuity locations.

For organizations that use a separate devolution plan from the continuity plan, include the baseline information in this section in the organization continuity plan and include a reference to the devolution plan in the appropriate places within this section.

Continuity Planning
Decision Process When Incident Occurs

SAMPLE: Conceptual Executive Decision Process Matrix for Continuity



From: Continuity of Operations Plan Template for Federal Departments and Agencies
https://www.fema.gov/sites/default/files/2020-07/COOP-Planning-Template_091813.pdf

Continuity Planning Responsibilities

SAMPLE: Continuity of Operations Responsibilities

The following table shows examples of some Continuity of Operations responsibilities.

Position	Responsibilities
Director	• Provide strategic leadership and overarching policy direction for the Continuity program • Implement the Continuity Plan when necessary or directed • Update/promulgate Orders of Succession and Delegations of Authority • Ensure adequate funding is available for emergency operations • Ensure all components participate in Continuity exercises • Update Continuity Plan annually
Communications Specialist	• Update telephone rosters monthly • Conduct alert and notification tests
Records Specialist	• Review status of essential files, records, and databases
Training Specialist	• Develop and lead Continuity of Operations training • Plan Continuity of Operations exercises
Continuity Personnel	• Be prepared to deploy and support organization Essential Functions in the event of a Continuity Plan implementation • Provide current contact information to their manager • Know role and responsibilities in the event of Continuity Plan activation • Participate in Continuity training and exercises as directed • Have a telework agreement for this position, if applicable

From: Continuity of Operations Plan Template for Federal Departments and Agencies
https://www.fema.gov/sites/default/files/2020-07/COOP-Planning-Template_091813.pdf

Continuity Planning Resources

There are a number of resources ***available for free*** that can help you with your planning.

- NIST SP 800-34 Rev.1: Great info and templates. But first timers and small communities, it has a lot of information to digest
- Continuity of Operations Plan Template and Instructions for Federal Departments and Agencies July 2011: Designed for Federal Gov but still applicable.
  60-page template; again, it may be a bit much for beginners.
- Continuity of Operations An Overview:
  FEMA brochure with contact info
- Continuity of Operations Planning:
  (Texas) State Office of Risk Management (SORM), has links to guidance and templates
  - https://www.sorm.state.tx.us/coop

CIAS-ISAO
Community Cybersecurity Program

Mission: The core mission of the CIAS-ISAO is to help states, local jurisdictions, tribes, and territories to establish a comprehensive cybersecurity program by using the state-supported Community Cyber Security Maturity Model (CCSMM).

TX ISAO role: Community Awareness, Preparation and Prevention

CIAS-ISAO: WE ARE HERE TO HELP!

- Training & Exercises
- Culture of Cybersecurity & K-12 Educational Cybersecurity Program
- Customized Cybersecurity Competitions
- Assessments
- ISAO support for communities
- Establishing and Growing a Program (CCSMM)

CIAS-ISAO
COMMUNITY CYBERSECURITY PROGRAMS

UTSA

Questions?

Julina Macy
Director of Communications
Julina.Macy@utsa.edu

Gregory White, Ph.D.
CIAS Director
Greg.White@utsa.edu

CIAS-ISA
COMMUNITY CYBERSECURITY PROGRAMS

UTSA