Department of Administrative Services

State Business Continuity Program Guidance

February 2025

Table of Contents

I. Executive Summary 4
II. Purpose 4
III. Assumptions 5
IV. Program Management 5
A. Vision 6
B. Measures of Success 6
C. Programmatic Authority 6
1. Executive Management 7
2. State Business Continuity Steering Committee 7
3. State Business Continuity Program 8
4. State Business Continuity Manager 8
5. Agency Business Continuity Coordinators 9
6. Agencies, Departments, Boards, and Commissions 9
D. Programmatic Approach 9
1. Agency-level Procedures 9
V. Guiding Principles 10
VI. Stakeholders 10
VII. State Essential Functions 11
VIII. Planning Process 12
A. Risk Assessment 13
1. Conducting a Risk Assessment 13
2. Risk Assessment Organizational Change Management 13
3. Risk Assessment Process Illustration 15
B. Business Impact Analysis 16
1. Support of Agency Mission Essential Functions 16
2. Conducting the BIA 16
3. BIA Organizational Change Management 17
4. BIA Process Illustration 17
C. Risk Reduction Strategies 18
D. Recovery Strategies 18
1. Immediate 18
2. Short-Term 18

3. Long-Term 18

IX. Plan Development 19

A. COOP Structure 19

1. Orders of Succession 19
2. Delegations of Authority 19
3. Alternate Work Locations 19
4. Continuity Communications 21
5. Essential Records Management 21
6. Human Resources 22
7. Devolution of Control 22
8. Reconstitution Operations 23
9. Supporting Appendices 23

B. Plan Development Illustration 23

X. Testing, Training, and Exercise 24

A. Testing 24

B. Training 25

C. Exercise Methodologies 25

1. Structured Walk-through Exercise 25
2. Tabletop Exercise 26
3. Functional Exercise 27
4. Full-Scale Exercise 28

XI. Maintenance, Awareness, and Measurement 29

A. Required General Maintenance 29

B. Program Awareness 29

C. Program Measurement 30

XII. Authorities and References 30

XIII. Attachments 31

A. Available Planning Templates 32

B. Self-assessment Maturity Checklist 33

C. Terms and Definitions 35

D. Record of Changes 42

I. Executive Summary

Ohio's State agencies are responsible for an array of essential functions upon which our citizens rely. In the event of a disruption, these are functions that need to be resumed quickly in order to prevent a number of dire consequences from being realized. Service resumption by State agencies largely depends upon the existence of comprehensive, updated continuity of operations (COOP) plans that detail how the agency will operate and recover after a disruption. Continuity of operations, as defined in the National Security Presidential Directive-51/Homeland Security Presidential Directive-20 (NSPD-51/HSPD-20) and the National Continuity Policy Implementation Plan (NCPIP), is an effort within individual agencies to ensure that the State's and the agency's mission essential functions (MEFs) continue to be performed during a wide range of events, including localized acts of nature, accidents, and technological or attack-related emergencies. All State agencies, departments, boards, and commissions should have COOP plans and continuity of government (COG) capabilities in place *before* an emergency occurs to ensure that emergency response actions are taken as quickly as possible. This combined planning concept (COOP/COG) will be referred to as business continuity for the purposes of this document.

II. Purpose

This document provides State agencies, departments, boards, and commissions with a common framework for planning, executing, and maintaining individual COOP programs, which in turn roll up into a larger State Business Continuity (BC) Program, managed by the Ohio Department of Administrative Services (DAS), Office of Collective Bargaining (OCB). The planning processes outlined in this guidance document may be used to identify, plan, and manage any disruption to normal business operations. The term "critical event" will refer to a disaster, emergency, incident, or any other hazard that may disrupt normal business operations. This guidance document is not intended to provide a comprehensive set of standard operating procedures (SOPs), management instructions, or a detailed review of generally accepted practices. Individual planning efforts must occur at the agency level.

The State BC Program was established to achieve the following objectives:

- Development of uniform business continuity processes, supporting the timely resumption of internal (agency) and external (State) mission essential functions across the enterprise.
- Assist agencies in the identification and prioritization of mission essential functions and dependent business processes and systems.
- Standardize response and recovery efforts across the State.
- Build an infrastructure that provides continuity planning tools and templates for agencies to leverage in developing their own respective programs.
- Establish integrated operations, planning, and decision-making processes for continuity of operations across the State.

III. Assumptions

The State BC Program has been built upon the following planning assumptions:

- State agencies, departments, boards, and commissions, which will singularly be referred to as "agencies", will assign a BC Coordinator to work with the State BC Manager in the DAS OCB Business Continuity Program
- Agency BC Coordinators will be empowered by their respective management teams to represent their agency in BC Working Groups and to develop templates, policies, training, and exercises on behalf of their agency.
- Agencies will create after-action reports (AARs) and revise plans to strengthen areas of improvement identified in exercises and during critical events.

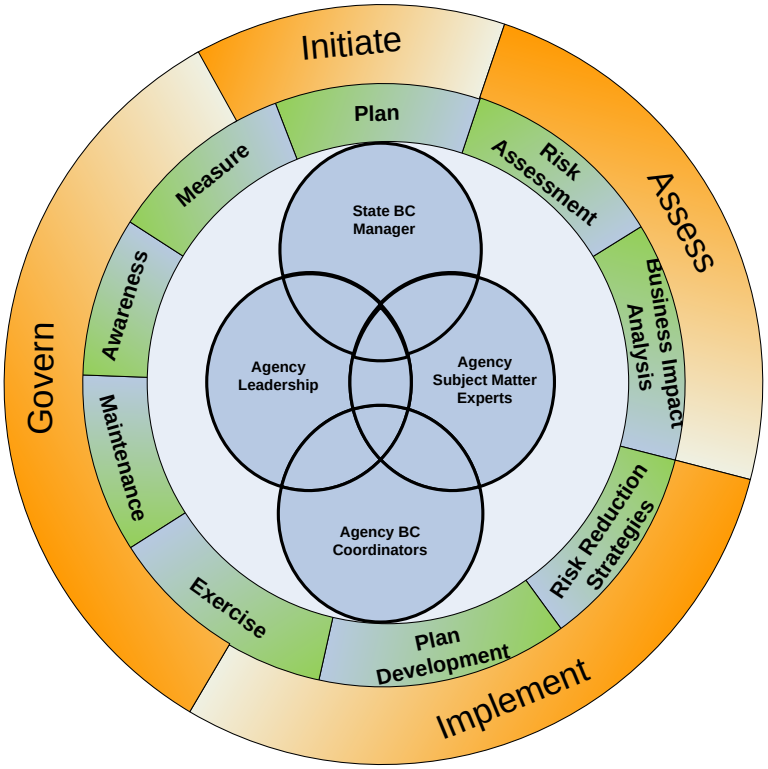
IV. Program Management

The DAS OCB Business Continuity Program is committed to providing its stakeholders with a comprehensive business continuity program, including policies, procedures, standards, planning and implementation templates and tools, and risk identification and mitigation strategies. The State BC Program was developed with and will continue to be improved upon through collaboration with State agencies, as is evidenced by the multi-agency BC working groups and agency-level BC Coordinators. Agency expertise is highly valued and vital to the program's successful implementation and maturation.

The framework of the BC Program includes the following elements:

- Vision
- Governance
- Approach
- Policy, Standards, and Procedures

The diagram to the right illustrates the interdependent and continuous nature of business continuity planning.



A. Vision

The vision of the State of Ohio Business Continuity Program is to sustain and improve upon a comprehensive State business continuity program, that works to ensure the safety of the public and the continuation of the State of Ohio's mission essential functions during an emergency, therefore promoting resiliency in the aftermath of service disruptions.

This implements a sustainable program to identify, assess, prioritize, manage, control, and minimize risks that could potentially impact normal business operations specifically regarding employee safety, citizen impact, business resumption, and property impact. The primary focus is to protect employees, minimize the impact on citizens, and protect State property during a critical event.

B. Measures of Success

The State BC Program is designed to ensure that mission essential functions that support those services critical to the citizens of Ohio and the long-term viability of the State are maintained before, during, and after an interruption to business operations.

The following measurements will be indicative of this program's success:

- Identification and prioritization of state essential functions (SEFs).
- Establishment of a command-and-control structure to be used during an incident.
- Creation and maintenance of a portfolio containing current, comprehensive COOP plans for all State agencies.
- Creation and maintenance of a COG plan, based on agency COOP plans and the State mission essential functions.
- Development of a framework for testing COOP plans to ensure that agencies' plans are viable and contain the state-identified core planning elements.
- Establishment and management of forums for state agencies to converse about and collaborate on business continuity planning efforts.
- Creation of a "culture of readiness", where State agencies and employees alike are conditioned to always be aware of threats to business continuity and proactively engage in COOP planning, testing of plans, and plan maintenance.

C. Programmatic Authority

Incidents may be local in nature or may have a statewide or regional impact, affecting multiple state-owned facilities and/or resources, rendering them partially or fully unavailable. For this reason, the State BC Program applies to all executive, judicial, and legislative branches and elected officials' business units, personnel, facilities, IT systems, services, and physical assets at all locations. The State Business Continuity Manager (BCM) will assist agency BC Coordinators in developing and managing their individual agencies' BC programs by providing the following assistance.

- Access to a standardized plan format.
- Use of a web-based BC plan development and maintenance tool (RPX).
- Guidance on conducting plan evaluations, testing, training, and exercises.
- Assistance in prioritization of essential functions, systems, and staff.
- Assistance in selecting alternate work locations.
- Facilitation of agency-to-agency interaction and coordination.

While the State BC Manager is tasked with establishing and managing the DAS OCB Business Continuity Program, the State Business Continuity Steering Committee provides overall guidance for the organization of business continuity from a state-wide perspective. However, every employee in every State agency has a responsibility to help define, implement, test, and maintain the program.

The State BC Program was developed using input and guidance from subject matter experts across the State. To ensure continuity of and consistency to the BC Program itself, these advisory responsibilities must not be delegated to others. This governance structure enables a holistic oversight to the State BC Program and contains the following support groups, discussed in the following sections.

1. Executive Management

Directors and executive-level staff of State agencies are accountable for BC program management and alignment with continuity policies, standards, procedures, and risk mitigation controls within their respective areas of responsibility.

2. State Business Continuity Steering Committee

Overarching BC guidance, support, and recommendations are provided by a multidisciplinary group, referred to as the State Business Continuity Steering Committee or BCSC. This group is responsible for providing input on, reviewing, approving, and endorsing State BC policy, objectives, and strategies. The members of this group agree to the roles and responsibilities defined for the State in the policies and procedures developed by the State BCM. The members of the BCSC will actively promote and provide business support for BC initiatives throughout the State.

This governance group is chaired and coordinated by the State BCM and includes representation from a selection of the State of Ohio's executive branch agencies. This Committee meets on a quarterly or as-need basis. The duration of member-agency engagement in the committee is a minimum of two years participation.

Members of the BCSC are funded by the member's home agency and are granted full voting rights of that agency. To ensure that all of the State's unique needs are met, members represent:

- Small agency (under 400 employees)
- Medium agency (400-1,500 employees)

- Large agency (over 1,500 employees)

Representatives serving on the BCSC are selected or assigned based on their overall knowledge of COOP, disaster recovery, public safety, and/or emergency response relative to their agency. Subject matter experts on State facilities management, finance, human resources, information technology, law, public relations, security, and other administrative functions are also incorporated into the BCSC by way of subcommittees and working groups.

3. State Business Continuity Program

Through the OCB State Business Continuity Program, DAS delivers business continuity and continuity of operations guidance and support to agencies by coordinating planning efforts across the State, therefore ensuring continuity of government.

This is accomplished by providing assistance in the planning, building, maintaining, and supporting of activities to ensure that agencies:

- Identify and mitigate operational risks that may lead to business disruptions *before* an incident occurs.
- Prepare for response to risks (natural, technological, and/or human-caused), both through the development and exercising of plans and through the engagement of essential employees, in a manner that demonstrates incident command and control.
- Recover and restore pre-identified, mission-essential business operations during and after an incident.

4. State Business Continuity Manager

The State BCM is responsible for the oversight of the DAS OCB Business Continuity Program and the planning, implementation, and maintenance of the overarching State BC program. The BCM ensures, in particular, that BC awareness is increased across the State. This is accomplished by:

- Marketing the program to the State and its county, city, and local counterparts.
- Working with State agencies to identify BC coordinators.
- Ensuring that the appropriate preparedness, response, and recovery policies, plans, procedures, standards, risk mitigation controls, and solutions exist and are made available to the State through the agency BC Coordinators.
- Recommending the methods to implement, encourage, and enforce BC policies.
- Developing tools to assist State agencies with continuity of operations plan and exercise development and implementation.
- Measuring and reporting on the level of compliance to such policies and overall program effectiveness to the State BCSC and Director of DAS.
- Advising the BCSC and the Director of DAS on preparedness, response, and recovery-related issues on a day-to-day basis.
- Serving as DAS's primary representative in interactions with external emergency management authorities and forums.

5. Agency Business Continuity Coordinators

COOP plan development and maintenance at each of the agencies is the responsibility of the agency's BC Coordinator. These individuals are assigned by their agency based on specific COOP, business continuity, facilities management, emergency management, and/or disaster recovery skills that they already possess or are in the process of acquiring. BC Coordinators must also be exempt staff, based on sensitive subject matter that may be discussed in the strike appendices of the COOP plans. Agency BC Coordinators will be empowered by their respective management teams to represent their agency in the development of State templates, policies, and trainings.

6. Agencies, Departments, Boards, and Commissions

All State Agencies, Departments, Boards, and Commissions (collectively known as "agencies") are expected to develop and maintain individual COOP plans to achieve the following goals:

- Provide the timely and orderly continuous performance of MEFs during and after an incident.
- Protect facilities, equipment, IT systems, records, and other assets that support MEFs.
- Reduce and/or mitigate disruptions to operations.
- Provide reconstitution or devolution of control after the incident is over.
- Minimize loss to the State.
- Prepare employees for response to and offer support to employees during critical events.

D. Programmatic Approach

The State BC Program identifies, assesses, prioritizes, manages, and controls risks that could disrupt normal operations, specifically by assisting agencies with:

- Reviewing COOP plans and programs.
- Analyzing the effect of critical events on business processes.
- Assessing risk to determine the severity and likelihood of threats that may occur.
- Identifying and implementing cost effective risk mitigation strategies.
- Including COOP planning within business process/systems development lifecycles.
- Developing strategies and procedures to maintain, resume, and recover SEFs and their respective supporting business processes.
- Validating documented plans through exercises.

1. Agency-level Procedures

Agency-level procedures must identify the supporting business processes of each mission essential function. Through documentation of these processes, the agency's BC program may

effectively and consistently analyze, assess, plan, review, implement, validate, and monitor COOP activities. Recovery procedures must document the actions necessary to respond to a critical event and restore MEFs. Procedures should address both immediate and short-term tasks and more time consuming, long-term tasks.

Recovery procedures will be documented using the guidelines defined in the COOP planning template. The business impact analysis, risk assessment, and recovery templates are designed to assist agencies in gathering critical and pertinent recovery requirements for the development of viable COOP plans.

V. Guiding Principles

Business Continuity is an operational risk-management discipline that addresses the preservation of continuity of operations and continuity of government. This effort is established via a hierarchical set of policies and procedures that help agencies and business managers define and mitigate risks, and respond to and recover from interruptions, while maintaining a balance between business value and risk mitigation costs. BC policies are high-level documents used to put continuity planning principles into practice. Procedures are sets of established standards and activities aimed at achieving defined objectives in a measurable and repeatable manner across the State.

The DAS OCB Business Continuity Program has identified the following guiding principles to further assist State agencies in the development of a comprehensive State BC Program.

- Business continuity will be built into the State's business operations.
- Guidance from the BCSC will be communicated to State agencies by the State BCM.
- Agencies will develop individual COOP plans.
- Business impact analyses and risk assessments will be conducted by the agency based on a pre-determined schedule set forth in the agency's COOP plan.
- After development, COOP plans will be consistently maintained and exercised.
- Training and exercises will be conducted to familiarize all of the agency's key stakeholders with COOP plans.
- All extraneous statutory requirements will be followed during planning and execution of the BC program.
- The BCSC will make programmatic recommendations to the DAS OCB Business Continuity Program
- The DAS OCB Business Continuity Program will identify and recommend standards and planning templates for use by State agencies, on the behalf of the BCSC.
- Executive oversight and guidance will be provided by the Business Continuity Steering Committee, chaired by the DAS BCM.

VI. Stakeholders

The stakeholders for this program include:

- Leadership of State Agencies
- The Governor of the State of Ohio
- Executive, Legislative, and Judicial Branches of Government
- Publicly Elected Officials
- State of Ohio employees
- Residents of Ohio
- Federal and local government agencies
- IT systems and service providers
- Private-sector partners

VII. State Essential Functions

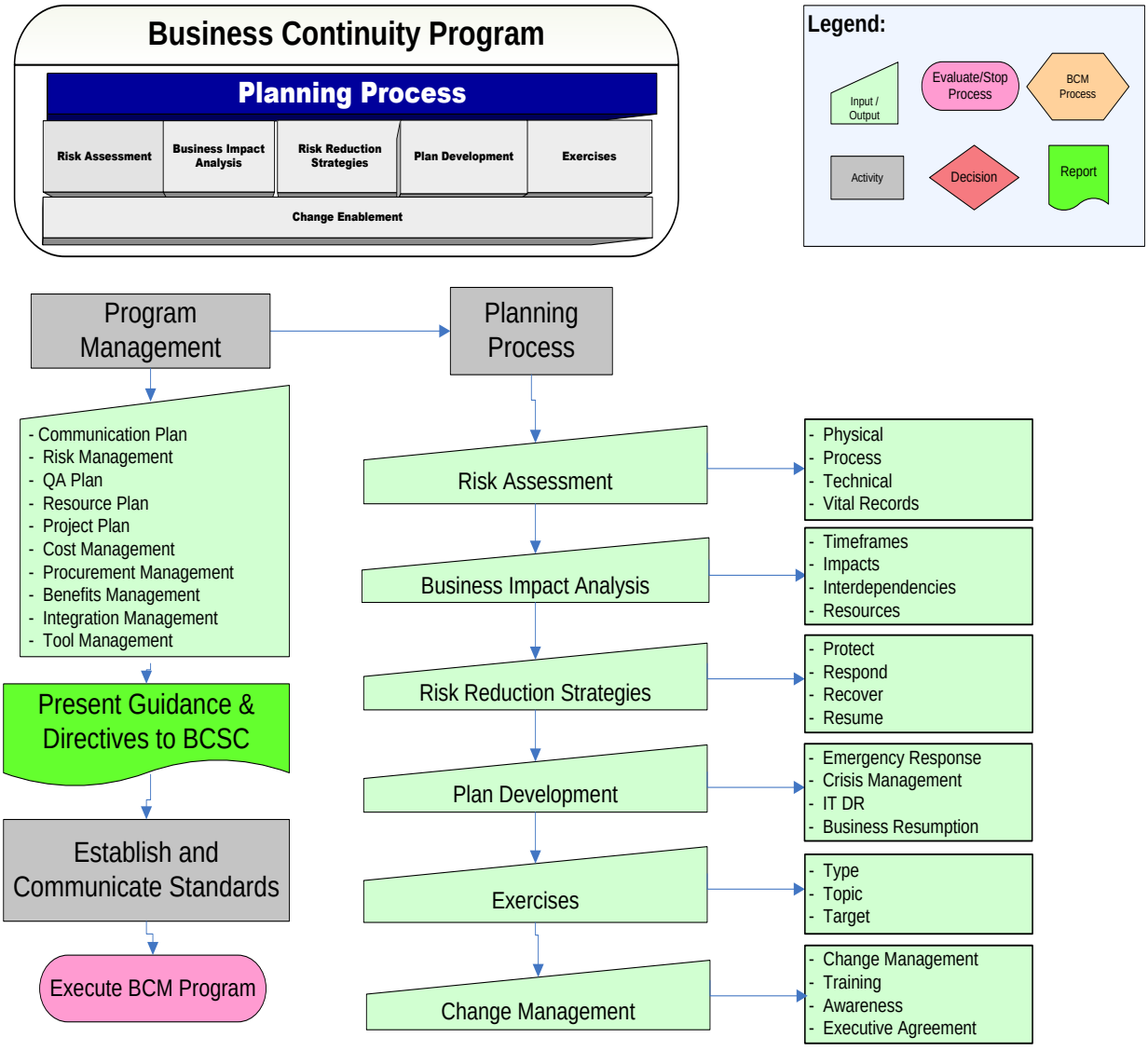
The following State Essential Functions (SEFs) were developed based on the analysis of existing state and federal planning documents, administrative cost, existing response plans, information technology disaster recovery planning priorities, and other States' best practices/lessons learned. These functions were created to assist the State of Ohio in identifying functions essential to the continuity of operations across the enterprise. Descriptions of each SEF are included in the table below.

FUNCTION	DEFINITION
Maintain Civil Law and Order	Maintain civil law and order in the state of Ohio, by preventing crime and protecting and defending the state, its people, and its critical infrastructure against attack.
Provide Essential Services to the Public	Provide essential services that address the health and safety needs and public welfare of the state and its citizens, including but not limited to: firefighting, search and rescue, hazardous materials response, emergency management and disaster recovery, emergency medical services, healthcare, custodial care of institutionalized populations, as well as assistance in locating food and shelter.
Ensure Availability of Critical Infrastructure	Ensure the availability of communication infrastructure, drinking and potable water, environmental protection services, energy/power, financial services, sanitation, and transportation networks.
Ensure Continuity of Government	Ensure the continued functioning of government by providing for succession to key positions, organizational communications, management of operations, personnel accountability, and a visible leadership structure, while continuing to meet legal and/or statutory requirements.
Ensure Economic Stability	Protect Ohio's economy by providing for the solvency of government and the stability of financial institutions and systems.
Offer Resource and Logistical Support to Agencies	Offer and provide resource and logistical support and assistance to federal, state, local, and their non-profit partners.

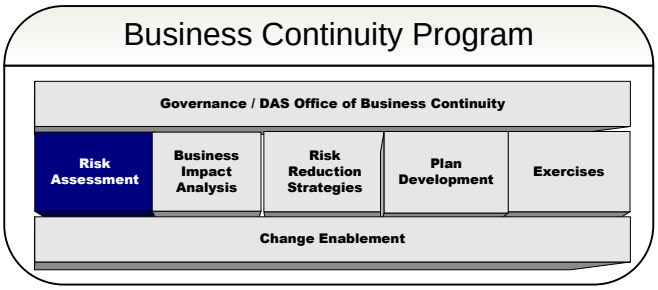
VIII. Planning Process

The planning process provides a conceptual model of the steps that should be taken throughout the Business Continuity Planning (BCP) process. This model presents guidelines for agencies to follow in developing a comprehensive COOP program. The process was developed by analyzing best practices from other state and national organizations, existing State and Federal guidance, existing emergency response practices, administrative cost analysis, existing emergency response plans, and information technology disaster recovery planning priorities.

There are several key stages to the BCM approach. The description of each stage is based on the generally accepted practices and guidance from the Disaster Recovery Institute International (DRII) enhanced to meet the planning needs of each agency. This planning framework reinforces repeatability, adaptability, and proactive activities. The following diagram illustrates the BCP process flow.



A. Risk Assessment



Before a business impact analysis (BIA) may be conducted or a COOP may be developed, the agency must first know what physical risks are likely to affect their business operations. The objective of a risk assessment (RA) is to:

- Identify and document the threats, scenarios, and environmental surroundings that are most likely to adversely affect the agency's MEFs and facilities.
- Evaluate the potential for damage.
- Define and implement controls necessary to prevent or minimize the effect of the potential losses.
- Evaluate the effectiveness of the controls.

The agency will make certain that a RA is conducted to determine the severity and likelihood of realistic threat scenarios and will make certain that the RA includes a gap analysis to determine what is necessary in order to achieve the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) identified in the BIA.

1. Conducting a Risk Assessment

The agency BC Coordinator will work with the Risk Management Team and other key stakeholders to gather and analyze data for determining the threats, scenarios, and environmental surroundings that are most likely to adversely affect the agency's MEFs and facilities, including the damage that such incidents may cause and the controls needed to prevent or minimize the effects of potential loss. The following steps will be taken to perform the RA.

a. Identify potential risks based on probability, exposures, loss potentials, and consequences/impact by using the State-identified risk assessment tool (spreadsheet and wizard).
b. Identify risk reduction/mitigation activities and alternatives, and controls and safeguards to prevent or minimize the effect of the loss.
c. Evaluate the effectiveness of controls and safeguards.
d. Identify external expertise and assistance required.
e. Present summary of information to agency leadership for confirmation of realistic levels of risk.
f. Implement security-related measures and procedures to fill any unacceptable gaps in risk control.

2. Risk Assessment Organizational Change Management

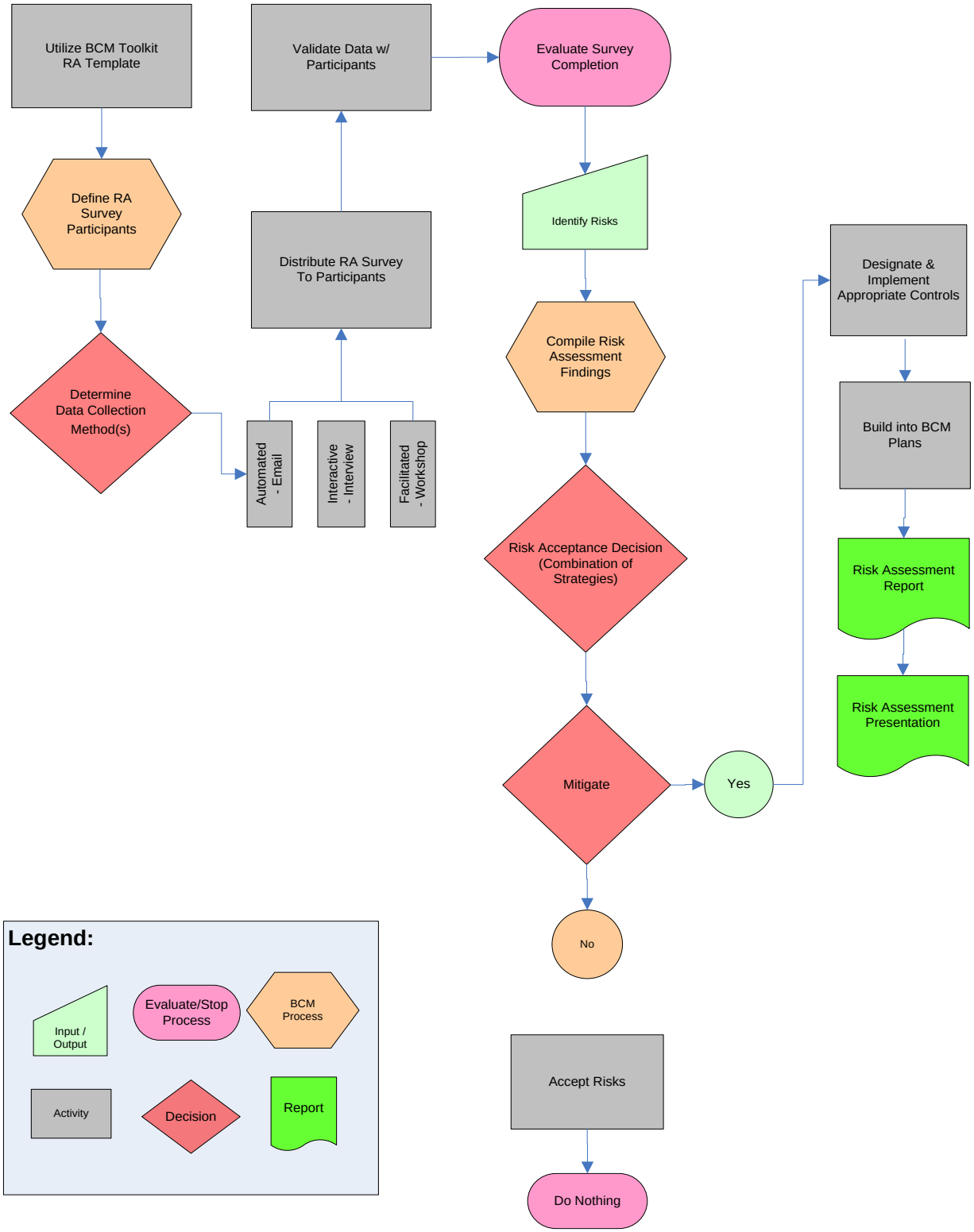
The agency will make sure that when a new business process is being implemented or a new facility is being built, an individual RA will be conducted on the business process or facility prior to the annual plan submittal. In addition, the agency RA will be reviewed and updated annually to ensure that any changes in risk are captured in the COOP.

Additionally, if the agency is located in one of the state-owned facilities (listed below), the agency BC Coordinator will ensure that the agency's facility security specialist is working with the DAS, General Services Division (GSD), Office of Properties and Facilities, to manage building security access. Primarily, this interface will occur by way of quarterly submission of on-boarding/off-boarding records for agency employees to the DAS GSD State Building Security Administrator. Agencies will continue to be responsible for maintaining and following existing procedures for day-to-day security of their respective systems. Again, this caveat only applies to agencies in the following, state-owned locations; all other agencies are fully responsible for building security access.

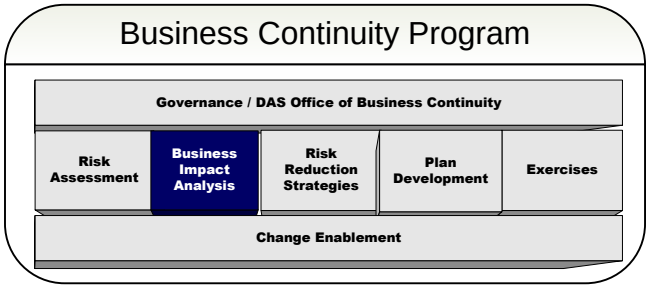
- 25 S. Front St., Columbus, OH 43215
- 4200 Surface Rd., Columbus, OH 43228
- A. B. Graham Building, 8995 E. Main St., Reynoldsburg, OH 43068
- Lausche State Office Building, 615 W. Superior Ave., Cleveland, OH 44113
- North High Complex, 246 N. High St. and 35 E. Chestnut St., Columbus, OH 43215
- Ohio Governor's Residence and Heritage Garden, Bexley, OH 43209
- Rhodes State Office Tower, 30 E. Broad St., Columbus, OH 43215
- Riffe Center for Government and the Arts, 77 S. High St., Columbus, OH 43215
- State of Ohio Computer Center, 1320 Arthur E. Adams Dr., Columbus, OH 43221

The rest of the page has been intentionally left blank.

3. Risk Assessment Process Illustration



B. Business Impact Analysis



Before a comprehensive COOP plan can be developed, a BIA must be performed by the agency's BC Coordinator and key agency personnel to identify the wide-ranging adverse impacts that could result from an incident and to prioritize key business processes.

In this planning stage, analytical techniques and tools are used to quantify and qualify the business impacts to the agency. This includes activities associated with assessing the effects of disruptions to normal business operations, defining criticality, prioritizing the business processes, and determining recovery timeframes and resource requirements.

The BIA includes:

- Identification of the potential impact of uncontrolled and unexpected incidents.
- Estimation of the recovery time objective (RTO) and the data, operations, and financial loss tolerances.

1. Support of Agency Mission Essential Functions

The agency will make certain that the BC Coordinator conducts a BIA in conjunction with key agency leadership to determine critical business processes that support the agency's MEFs. Agency MEFs can also be described as specific services that the agency performs that support the SEFs.

2. Conducting the BIA

After the BC Coordinator and leadership team have determined the agency MEFs, the following steps will be taken to perform the BIA itself. At a minimum, agencies should complete the BIA "heat map"; agencies with more mature BC programs may choose to leverage the more in-depth, long-form interview format BIA instead. Both options are available on the State BC website.

a. Identify departments, business processes, owners, technology, and facilities that support each MEF. The agency will identify knowledgeable subject matter experts or key agency stakeholders that support each agency MEF for participation in the BIA process. The BC Coordinator will facilitate the BIA development process and assist the BIA development team in determining the financial and non-financial impacts that an incident could have on the operation of their agency.
b. The BC Coordinator will complete each field or tab of the State-identified BIA planning tool (spreadsheet and/or wizard) with the assistance of the BIA development team. This process may take up to three months.

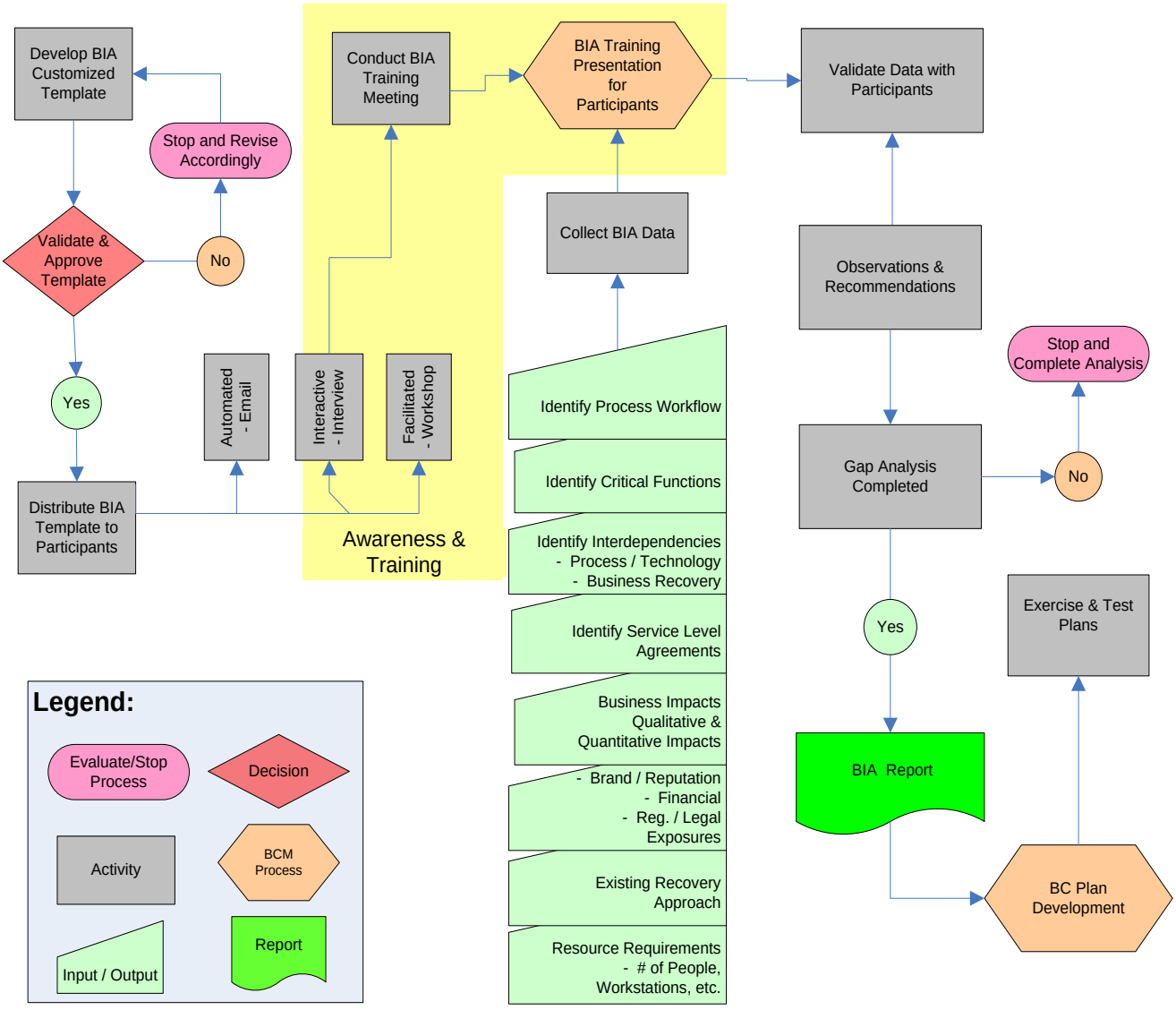
c. Agency leadership will confirm and sign off on the BIA results, including resulting MEFs and RTOs. The DAS OCB Business Continuity Program may assist agencies in analyzing the results of the BIA to determine what resources are needed to achieve RTOs.

3. BIA Organizational Change Management

The agency will make sure that when a new business process, function, or system is being implemented, a BIA is conducted on the business process, function, or system prior to the annual plan submittal.

In addition, the agency BIA will be reviewed annually to ensure that any changes in business impact are captured in the COOP.

4. BIA Process Illustration



C. Risk Reduction Strategies

The DAS OCB Business Continuity Program encourages proactive management of potential risks to the agency before these risks become a reality. The agency recognizes the need to invest in a cost effective BCM Program; the objective being to identify and select the alternative business continuity strategies that will maintain agency MEFs. To accomplish risk reduction strategies, the DAS OCB Business Continuity Program asks that agencies perform the following:

- Review alternatives, advantages, disadvantages, and cost including mitigation as a recovery strategy.
- Identify viable recovery strategies within Divisions.
- Consolidate and integrate recovery strategies.
- Identify off-site requirements and alternate sites.
- Develop process-specific standard operating procedures.
- Demonstrate commitment from management for developing, implementing, and updating strategies.

D. Recovery Strategies

The following recovery strategies are not hazard specific, but do address immediate, short-term, and long-term recovery tasks, which may be initiated during any type of incident.

1. Immediate

Immediate recovery strategies identify tasks that should be performed as soon as possible following an incident in order to reduce possible impacts. In many instances, these strategies will address initial communications to clients and other business contacts, and response required of critical business functions.

2. Short-Term

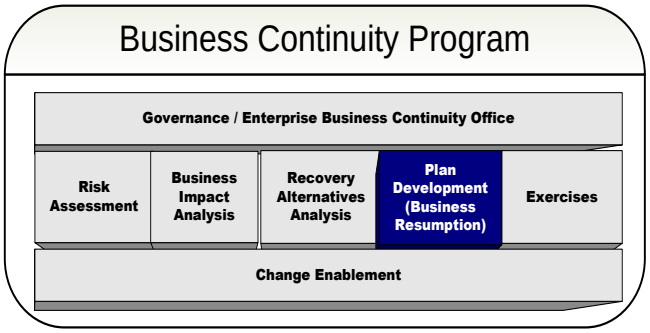
Short-term recovery strategies identify alternate options which may be implemented following a short-term telecommunications or computer service outage. Similar to the immediate recovery, these strategies may also be used to reduce business impacts following a catastrophic disaster until long-term recovery strategies can be implemented.

3. Long-Term

Long-term recovery strategies address a worst case scenario such as total destruction or loss of access to the home site, resulting in an extended business interruption. Long-term strategies address recovery at an alternate site using resources obtained by Business Continuity Management.

IX. Plan Development

The objective of this phase is to incorporate the data obtained through the RA, BIA, and identification of risk reduction strategies into the development of the agency's COOP Plan. This includes defining recovery management and control requirements, defining the format and structure of plan components, and developing supporting appendices. Design of the COOP is accomplished by leveraging the State-identified COOP template to:



- Identify and assign key staff to each stage of the planning process.
- Develop processes to update and maintain the COOP in accordance with the State BCSC and DAS OCB Business Continuity Program's strategic direction.
- Defining a maintenance schedule, requirements, and process.
- Developing and implementing change management procedures for COOP updates.

A. COOP Structure

The COOP plan focuses on sustaining the agency's MEFs during and after an incident. Systems and applications are considered in the COOP plan in terms of their support to the MEFs. The COOP base plan discusses general continuity of operations activities that apply across all-hazards, while its supporting appendices contain more detail specific to a pre-identified hazard or scenario. Agencies are encouraged to tailor these appendices to meet their respective organizational needs.

1. Orders of Succession

Orders of Succession identify and determine succession of personnel staff that will take command during and/or after an incident, if agency leadership is incapacitated or unavailable. Pre-establishing this chain of command enables an orderly transition of leadership, while also ensuring that respective successors are able to be cross-trained on duties in advance.

2. Delegations of Authority

For a rapid response to most any incident, agencies must identify and document the delegation of authority to make policy determinations and decisions for key leadership positions at the various organizational levels (i.e., headquarters, regional, field, etc.) and locations, as appropriate. This grants succeeding personnel with the authority needed to perform their duties.

3. Alternate Work Locations

If the critical event renders the primary work location unusable or unreachable for longer than the shortest RTO, it may become necessary to transition business operations to an alternate work location (AWL). AWLs are workspaces that are geographically separated (5 miles or more away) from the primary workplace so that they are not likely to be impacted by the same disruptive events that affect the primary worksite. Separate risk assessments should be conducted on all prospective AWLs to determine the most likely threats to the alternate locations; AWLs should not share the same vulnerabilities as the primary facility.

Options such as moving essential staff to another, pre-identified facility owned or leased by the agency; co-locating with another agency; working remotely from a home office, satellite office, or other location outside of the primary work location. Multiple types of AWLs may be used. A portion of the primary work location may even continue to be used if the incident commander and/or architect has determined that it is safe.

a. Requirements

- Adequately accommodate the staff and equipment necessary to conduct essential functions. This includes the continuity response team, support teams, and any other essential staff.
- Be located a sufficient distance from the primary facility to avoid being encompassed by the same physical risks/hazards.
- Be identified ahead of time so that valuable recovery time is not spent hunting for a place where work can be done.
- Have documented memorandums of understanding (MOUs) or mutual-aid agreements (MAAs) if the AWL is co-located with another agency or organization. Sample AWLs MOUs are discussed in more detail in section 9.1.3.3 of this document.
- If the employee is using a documented telework location, the risk associated with using a home office should be included in the telework agreement. See DAS Teleworking Policy HR-32 for more information.

As much as possible, the AWL should offer the systems and configurations that are used in normal, daily activities, including:

- Communications.
- IT equipment, software, network, and internet access.
- Hard copy records access.
- Logistical support such as hotels, restaurants, gas stations and services within convenient proximity.
- Ability for workers to commute or provision of transportation.
- Emergency back-up power capability.

b. Types

RTO requirements should be used to determine the advance setup required at the AWL. One of the following site types may be considered.

- Hot Site – all information and communications systems, infrastructure, security, and access needs are in place at the site before the time of need. This may be the best choice if the agency has multiple offices/facilities.
- Warm Site – some of the equipment and infrastructure is stored and maintained to allow more rapid resumption of work.
- Cold Site – It may be necessary to install equipment and access upon arrival.

c. MOUs and MAAs

The DAS OCB Business Continuity Program has samples of AWL MOUs/MAAs that agencies may use. At a minimum a contract should be agreed upon that clarifies the following:

- Hours of operation.
- Security and parking access requirements.
- Availability of power, telephone, and computer outlets.
- Internet access and bandwidth availability.
- Break room, restroom, and other common use space accessibility.

4. Continuity Communications

An effective communications systems needs to be established that supports full connectivity, under all conditions, among key agency leadership, divisions, field offices, other agencies, critical customers, and the public so that agency MEFs continue to be performed during an incident.

5. Essential Records Management

An agency's official essential records program must be developed before an incident to protect the records required to continue agency MEFs at an AWL and ultimately, resume normal operations.

a. Record Retention Policy

An agency COOP plan is meant to serve as a "living" document. As the COOP plan, its supporting appendices, job aids, standard operating procedures, and other applicable documentation are revised, updated, and replaced by more current documents, the former versions may be destroyed. This will reduce confusion over the currency of instruction and ensure that all employees are following the same planning version.

b. Public Record Exemptions

Although certain sections of the COOP plan, appendices, and supporting documentation may be open to public record requests, the release of the following information may be exempt:

- Infrastructure Records – defined by Ohio Sunshine Laws as, "…any record that discloses the configuration of a public office's "critical systems", such as its communications, computer, electrical, mechanical, ventilation, water, plumbing, or security systems."
- Security Records – defined by Ohio Sunshine Laws as, "…any record that contains information directly used for protecting or maintaining the security of a public office against attack, interference, or sabotage to prevent, mitigate, or respond to acts of terrorism."

Agency BC Coordinators are advised to review all public record's requests with their respective legal counsel to determine if COOP information may fall under one of the exemptions listed above.

6. Human Resources

Continuity leadership and response team staff must be identified, recorded in the COOP, and briefed on their role *before* an incident occurs. For the purposes of this document, these employees will be referred to as "essential employees". Per State of Ohio Administrative Policy HR-11 Public Safety Emergency Procedures, by October 1st annually, each agency must review and update a listing of essential employees expected to work during a public safety emergency. These employees must also be predesignated in the Ohio Administrative Knowledge System (OAKS) and notified of their responsibilities before, during, and after an incident.

Additionally, if the agency is located in one of the state-owned facilities identified in the Risk Assessment section of this document, the agency BC Coordinator will ensure that the agency's facility security specialist is working with the DAS, General Services Division (GSD), Office of Properties and Facilities, to manage building security access. The facility security specialist will coordinate the following activities on behalf of the agency:

- Building Security Access Badging on a daily basis
- Reviewing Building Security Access on a quarterly basis
- On-boarding/off-boarding of employees to the security system
- All other extenuating circumstances (e.g., same-day access termination)

Lastly, this section of the Plan should discuss any back-up methods of processing that would be activated with the COOP to support essential HR activities, such as payroll, scheduling, benefits, hiring/terminations, etc.

7. Devolution of Control

Devolution of Control refers to the transfer of functions and responsibilities from the primary staff to another office or location and staff, if it is deemed that the original office is ultimately unable to resume control of the service. The devolution plan and/or procedures must address the personnel and planning considerations needed to transfer performance of the MEFs and/or leadership authority away from the primary site and/or staff to a location that offers a safe and

secure environment. This section of the plan is only activated when an incident renders leadership and/or staff unavailable to or incapable of performing its MEFs.

8. Reconstitution Operations

Reconstitution refers to the process by which the agency's work force may resume normal operations at the original or replaced primary facility. This section identifies the reconstitution plan and/or procedures so that the agency is fully capable of accomplishing all MEFs and normal operations at the new or replaced facility once agency's leadership or their successors determine the alternate facility is no longer required.

9. Supporting Appendices

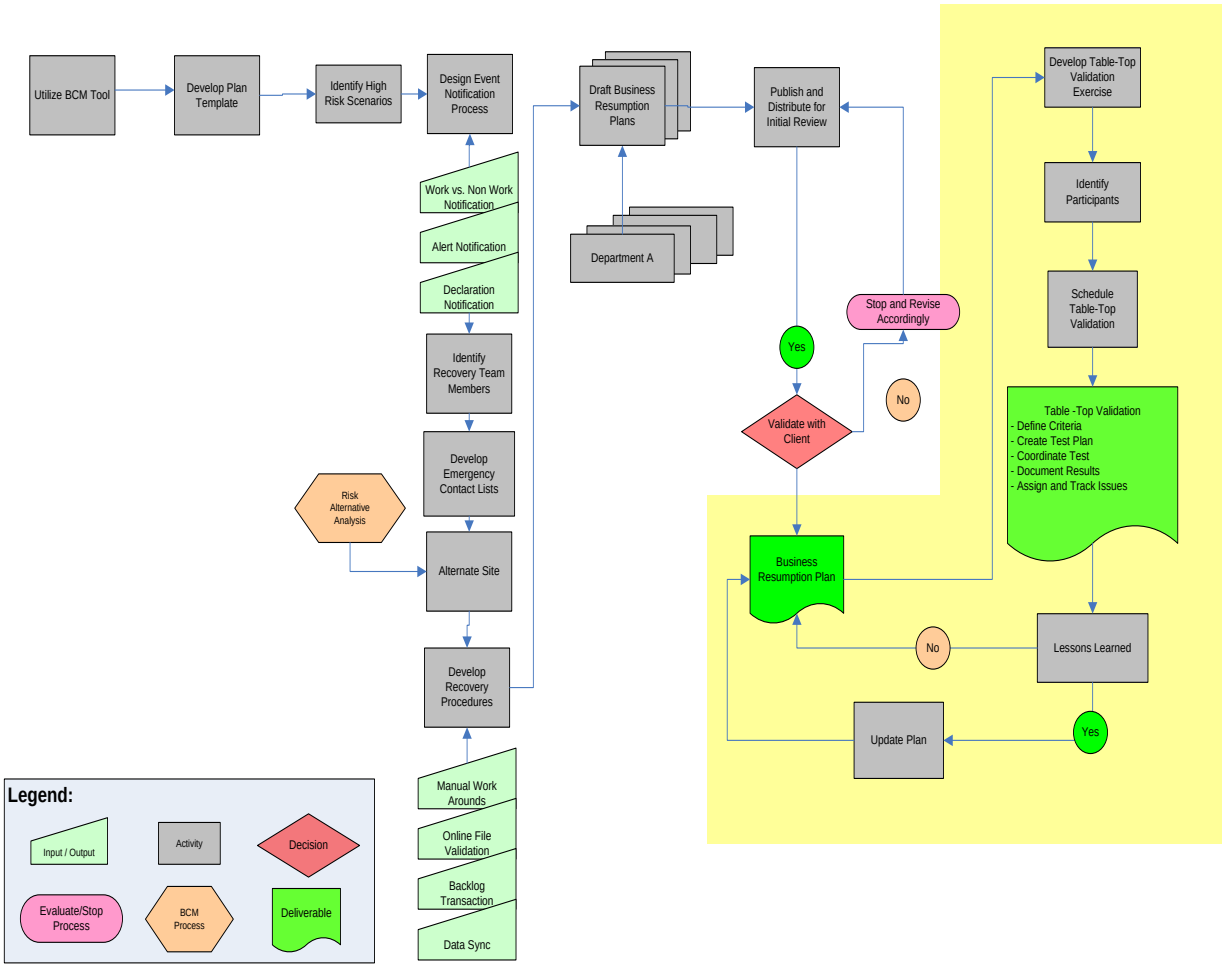
Specific appendices to the COOP plan address special planning considerations for key business processes or scenarios. The following appendices are a sampling of supporting documents that may be developed to further assist an agency in COOP planning. Each appendix is defined more in the terms and definitions attached to this document.

- Devolution of Control
- Emergency Relocation Group (ERG) Member Planning Guide
- Essential Records Packet
- Exercise Plans
- Facility Degradation Action Plan
- IT Disaster Recovery Appendices
- Multi-Year Strategy and Program Management Plan (MYSPMP)
- Pandemic Appendix
- Reconstitution Appendix
- Strike Appendix

B. Plan Development Illustration

The diagram on the following page illustrates the primary activities involved in the COOP plan development process.

The rest of the page has been intentionally left blank.



X. Testing, Training, and Exercise

For a BC program to stay current – and to enable management and staff to quickly respond to an incident – testing, training, and exercises must occur on an annual basis. Training provides the skills necessary for and familiarizes personnel with SOPs and tasks. Tests and exercises assess and validate all the components of the COOP, including the plan itself, policies, procedures, systems, and facilities.

A. Testing

Testing methods vary from minimum preparation and resources to the most complex. Each bears its own characteristics, objectives, and benefits. The type of testing employed by the agency may be determined internally or in consultation with each individual agency, based on that agency's specific resources, size, complexity, and nature of the test objectives; however, it is the goal of the DAS OCB Business Continuity Program that all State agencies reach at least Tabletop Top Exercise capacity. Please see the section of this document on Exercise Methodologies for more information on exercise types, levels, and methodologies.

B. Training

All members of the BC planning team should complete, at a minimum, the three basic COOP orientation courses from FEMA's Emergency Management Institute. The following training courses are available at no cost through FEMA's Independent Study website (http://training.fema.gov/is/):

1. IS-1300.a: Introduction to Continuity
2. IS-520: Introduction to Continuity of Operations Planning for Pandemic Influenzas
3. IS-545.a: Reconstitution Planning Course

Agency BC coordinators should take all recommended courses in FEMA's Continuity Excellence Series – Level 1 Professional Continuity Practitioner. For a full listing of COOP courses and/or certification requirements, please visit FEMA's Continuity Resource Toolkit (https://www.fema.gov/emergency-managers/national-preparedness/continuity) and select "National Continuity Training Program".

Agency staff that are involved in any portion of the COOP – from plan activation to recovery and reconstitution – should be trained on the role they play in ensuring the agency is able to continue its operations. Exercises serve as an acceptable outlet to test these employees and are discussed in more detail below.

C. Exercise Methodologies

There are several types of exercise methodologies that agencies may use to validate the COOP team's knowledge of and respective use of the agency's COOP plan and its hazard-specific appendices. Exercises may be performed under the guidance of agency-appointed exercise facilitators (i.e., the agency BC Coordinators, IT DR Coordinators and/or any other subject matter experts that are part of the COOP team) or by the State BCM upon request by the agency.

Typically, exercise types begin with the most basic methodology, becoming more robust as the agency's business continuity program matures. The DAS OCB Business Continuity Program has defined the following levels of exercise methodologies to be used under the State Business Continuity Program A description of each testing methodology, the purpose of each exercise, and how to perform the exercise are described in the sections below.

1. Structured Walk-through Exercise

a. Objective and Purpose

A Structured Walk-through Exercise is the most basic type of test. Its primary objective is to ensure that essential staff from all COOP sections and appendices are familiar with the COOP plan, associated tasks, and recovery procedures. The primary purpose of performing a Structured Walk-through Exercise is to validate the plan's completeness and process

documentation and to educate the interdependent COOP team members on test steps, tasks, and timeframes.

This type of exercise is characterized by:

- Discussion about the COOP plan in a small group setting.
- Individual and team training.
- Clarification and highlighting critical plan elements.

b. Performance

The following is a list of key steps involved with performing a structured walk-through exercise:

i. Gather key COOP team members (e.g., team leaders, alternate and recovery staff) for a short period of time to walk through a general, all-hazards response.
ii. Identify one or more written appendices to the COOP in chronological order;
iii. Discuss the appendix or section in terms of general format (order of recovery requirements as documented in the plan) and philosophy (prioritization of MEFs).
iv. Document any discrepancies, issues, and/or suggested revisions to the Appendix by way of an After-Action Report (AAR).
v. Develop a corrective action plan (CAP) based on the AAR.
vi. Update the appendix accordingly.

2. Tabletop Exercise

a. Objective and Purpose

A tabletop exercise (TTX) is somewhat more involved than a walk-through exercise because the participants choose a specific hazard scenario and apply the COOP to it. The primary purpose of this type of exercise is to validate the completeness of the documentation and to train the response members.

Components of a TTX include:

- Practice and validation of specific functional response capabilities.
- A focus on demonstration of knowledge and skills, as well as team interaction and decision-making capabilities.
- Role playing with simulated response at original and/or alternate work locations to act out critical steps, identify difficulties, and resolve problems in a non-threatening environment.

b. Performance

The following page includes a list of key steps involved in performing a TTX.

i. Gather multiple recovery teams (e.g. management, team leaders, alternate and recovery staff, etc.) for at least one hour in one location to discuss response actions taken in response to a specific, plausible scenario.
ii. Walk through several specific components of the COOP plan (e.g., written recovery procedures, MEFs, contacts, recovery strategies, etc.) in chronological order.
iii. Review and discuss the actions teams would take per their section of the COOP plan and recovery responsibilities.
iv. Discuss the COOP plan in terms of format (order of recovery requirements as documented in the plan) and philosophy (prioritization of MEFs) based on the defined scenario.
v. Document any discrepancies, issues, and/or suggested revisions for each plan component by way of an AAR.
vi. Develop a CAP based on the AAR.
vii. Update the COOP plan and its appendices accordingly.

3. Functional Exercise

a. Objective and Purpose

A functional exercise involves the actual mobilization of personnel to other sites to test communications and coordination as set forth in the COOP plan. This type of exercise is conducted on one or more components of the COOP plan under actual operating conditions. The primary purpose is to validate the completeness of the documentation, to train the COOP team members, and to document any additional requirements that may arise during the test.

Components of a functional exercise include:

- Demonstration of the response capabilities of several groups practicing a series of interactive functions, such as direction, control, assessment, operations, and planning.
- Actual or simulated response to alternate work locations or other facilities using actual communications capabilities.
- Varying degrees of actual, as opposed to simulated, notification and resource mobilization.

b. Performance

The following is a list of key steps involved in performing a functional exercise.

- Select the single and/or multiple component(s) of the COOP plan that will be tested.
- Define the scope, goals, and objectives for the exercise.
- Schedule the necessary timeframe to recover the COOP plan component, systems, application, and/or data.
- Mobilize personnel and resources to varied geographical sites, as necessary.
- Mobilize exercise players, COOP teams, and back-end users to the test location.
- Recover all pre-identified components, systems, applications, and/or data.

- Perform user testing as documented in the recovery procedures of the COOP plan in chronological order and according to test objectives.
- Document any discrepancies, issues, and/or suggested revisions for each COOP plan component by way of an AAR.
- Develop a CAP based on the AAR.
- Update the COOP plan accordingly.

4. Full-Scale Exercise

a. Objective and Purpose

A full-scale exercise (FSE) is the most comprehensive type of test that may be performed by an agency. In this type of exercise, the agency implements all or portions of its COOP Plan by processing data and transactions using back-up media at an alternate recovery site, typically under simulated operating conditions. FSEs generally occur over a longer period of time to allow scenarios to fully evolve, similar to how they would in an actual incident, and allow realistic role-play of all the involved groups.

The primary purpose of performing an FSE is to test the agency's ability to recover multiple, interdependent technical elements under conditions that mimic actual recoveries; to exercise communication and decision-making processes; and to test the adequacy of the COOP Plan documentation, recovery procedures, and resource knowledge involved.

Components of an FSE include:

- Validation of crisis response functions.
- Demonstration of COOP team knowledge and skills, as well as executive management response and decision-making capabilities.
- On-scene execution of coordination and decision-making responsibilities.
- Actual, as opposed to simulated, notifications, mobilization of resources, and communication of decisions.
- Conducting operations at actual alternate work locations or facilities.
- Statewide participation and interaction of internal and external response teams with full involvement of key business partners.
- Actual processing of data using backup media.

b. Performance

The following is a list of key steps involved with performing a Full-scale Exercise:

- Define the test scope, goals, and objectives for the exercise.
- Make certain that realistic conditions and activity volumes are set according to the recovery procedures documented in the COOP Plan.
- Use actual back-up media, systems, and date replication for testing.
- Invoke required vendor support.

- Schedule an exercise window (one to two days) with the necessary resources and support staff.
- Mobilize test participants, COOP and recovery teams, and the back-end users required for testing.
- Recover and test all Plan components identified in the scope of the test.
- Execute real-time transactions for each business unit participating in the exercise.
- Document any discrepancies, issues, and/or suggested revisions for each Plan component by way of an AAR.
- Develop a CAP based on the AAR.
- Update the COOP Plan and its Appendices accordingly.

XI. Maintenance, Awareness, and Measurement

The objective of this element of the BC program, accomplished at the more mature level of business continuity planning, is to establish the fundamental requirements necessary to validate COOP plan maintenance, employee awareness, and to measure the maturity of the State BC program and respective agency COOP plans.

A. Required General Maintenance

The following is a list of general maintenance required of the agencies:

- After a significant change to a business process, function, or system, a BIA will be performed for the business process, function or system prior to the annual plan submittal and plans will be updated accordingly.
- Within three months of an exercise or actual incident, the agency's COOP plan and its appendices will be modified, approved, redistributed, and made available on the State's business continuity planning tool, RPX.
- The COOP program will be reviewed on an annual basis following the respective COOP plan's maintenance schedule.
- COOP plan updates will be made directly to or uploaded to RPX to ensure that all team members have immediate access to the most recent version of the plan.
- One current, back-up copy of the COOP plan will be pre-staged at the agency's alternate work location(s). This back-up plan may be stored in electronic form on a USB drive or CD or hard copy in a three-ring binder. All advance staff will be informed, through annual tabletop exercise or upon receiving access to RPX, of where this COOP back-up is located at the AWL.

B. Program Awareness

To prepare the State's workforce for response to critical events, the DAS OCB Business Continuity Program recommends all agencies take the following steps to establish program awareness amongst employees:

- Establish objectives for the agency's COOP plan awareness and training program.

- Identify the functional awareness, training requirements, curricula, and audience for training.
- Develop methodologies, training tools, techniques, approaches, schedules, and materials suitable to the agency's employees.

The DAS OCB Business Continuity Program will work with each agency to determine what level of awareness should be built out and to assist agencies in developing their individual awareness programs.

C. Program Measurement

All agencies must perform an annual self-assessment of their respective COOP programs to ensure alignment to the policies, standards, and procedures that have been established in this document; however, an impartial review by DAS OCB Business Continuity Program may be performed as part of general auditing controls upon request.

The DAS OCB Business Continuity Program recommends the following steps to be taken toward self-evaluation of the agency's COOP program:

- Measure time since last exercise and number of unresolved issues.
- Measure time since last BIA was performed and immediacy to business processes/application changes.
- Review for completeness of COOP plan and exercise documentation.
- Review COOP plan for inclusion or elimination of new or obsolete business processes.
- Record and discuss number of unresolved issues.

This self-evaluation may be accomplished by using the Self-Assessment Maturity Model included in the attachments of this guidance document.

XII. Authorities and References

To follow is a list of Authorities and References sited in this document:

- Homeland Security Presidential Directive (HSPD)-20, Directive on National Continuity Policy, U.S. Department of Defense, May 2007
- National Security Presidential Directive (NSPD)-51, Homeland Security Presidential Directive, May 2007
- National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, U.S. Department of Commerce Joint Task Force, September 2020
- Continuity Guidance Circular (CGC), FEMA National Continuity Programs, February 2018 (2024 Update)
- Comprehensive Preparedness Guide 101, Developing and Maintaining Emergency Operations Plans, September 2021
- Devolution Planning Guidance, August 2019

- Emergency Management Standard, American National Standards Institute/Emergency Management Accreditation Program, May 2022
- Fact Sheet: Continuity and Reconstitution Planning Synchronization, FEMA National Continuity Programs, July 2023
- Guide to Continuity of Government for State, Local, Tribal, and Territorial Governments, FEMA National Continuity Programs, July 2021
- Guide to Continuity Program Management, FEMA National Continuity Programs, May 2020
- Ohio Administrative Code
- Ohio Revised Code
- Ohio Sunshine Laws Manual, Ohio Attorney General's Office, 2024
- Reconstitution Manager's Guide, FEMA National Continuity Programs, April 2023
- State of Ohio Administrative Policy HR-11, Public Safety Emergency Procedures, August 2023
- State of Ohio Administrative Policy HR-49, Critical Event Preparation and Response, September 2023
- State of Ohio Procurement Manual, March 2023
- Departmental, Division, and Office-level directives, policies, and standard operating procedures

XIII. Attachments

To follow is a list of additional planning documents:

- Available Planning Templates
- Self-Assessment Maturity Model
- Terms and Definitions
- Record of Changes

A. Available Planning Templates

Fillable, word documents of the following planning templates can be obtained either through the State's business continuity, web-based planning tool or by contacting the DAS OCB Business Continuity Program directly. PDF versions of these templates are also available on the OBC website (https://das.ohio.gov/employee-relations/office-of-collective-bargaining/business-continuity/1business-continuity). These templates were developed based on guidance from the Federal Emergency Management Agency (FEMA) Continuity Guidance Circulars (CGC), unless noted otherwise.

- Active Aggressor Response
- Agency COOP Plan
- Devolution of Control Appendix
- Disaster Recovery Plan – based on planning guidance from NIST
  - Low Risk Systems
  - Moderate Risk Systems
  - High Risk Systems
- Divisional COOP Plan
- Emergency Relocation Group Procedures
- Essential Records Plan Packet
- Essential Function COOP Plan
- Facility Degradation Appendix
- Exercise Appendices
  - Situation Manual
  - Tabletop Exercise
  - Telework Exercise
- Multi-Year Strategy Implementation Plan
- Pandemic Appendix
- Reconstitution Appendix
- Strike Plan

The DAS OCB OBC may be contacted at:

Ohio Department of Administrative Services
Office of Collective Bargaining
Business Continuity Program
Office 614-728-2884
BusinessContinuity@das.ohio.gov

B. Self-assessment Maturity Checklist

To follow is a basic checklist that may be used to gauge an Agency's maturity level. For mature agencies, a more robust assessment tool may be found on FEMA's Continuity Resource Toolkit (https://www.fema.gov/emergency-managers/national-preparedness/continuity) by selecting "Resources" and scrolling down to Continuity Assessment Tool.

☐ **Program *governance*, objectives, and plan format is in place.**

- A formal agency COOP plan and supporting appendices exist.
- Instructions regarding how to activate and use the COOP plan are documented.
- Additional information, such as scope, objective, and assumptions, is included in the plan.

☐ **A *business impact analysis and risk assessment* have been conducted.**

- A comprehensive BIA has been performed.
- A list of prioritized MEFs exists.
- An adequate level of process interruption insurance is established.
- Business process interdependencies are defined.
- Minimum recovery timeframes for all business processes are defined and documented.
- A comprehensive RA has been performed.
- Risk Strategy Gap Analysis has been developed.
- Identifiable risks have been addressed and mitigated.

☐ **A *declaration process* is in place.**

- Detailed procedures regarding how to activate the COOP plan are documented.
- Procedures for handling press releases and public relations, including a generic media statement, are included in the COOP plan.

☐ **Recovery *teams* have been identified and tasks have been assigned.**

- A location (i.e. EOC or AWL) where the response and recovery teams are to assemble during and after an incident to discuss recovery activities is clearly identified in the COOP plan.
- All recovery teams include appropriate key personnel and alternates.
- Detailed procedures for recovering MEFs and supporting business processes exist and are included in the COOP plan.
- Detailed procedures for restoring critical IT systems exist and are included in the COOP plan.
- Provisions for transportation of key personnel to an AWL(s) are included in the COOP plan.

☐ **Recovery *solutions and backup site(s)* are in place.**

- IT recovery solutions (e.g., hotsite, duplicate data center, etc.) has been developed and documented in the IT/DR appendices of the COOP plan.
- Key contacts affiliated with the AWL, and their phone numbers, are included in the COOP plan;
- Physical access controls exist at the AWL (e.g., keys, access cards, guard stations).
- Procedures for enforcing access restrictions for the network environment at the IT/DR site are in place and are included in the IT/DR appendices.
- Provisions for mail service at the AWL are in place and included in the COOP plan.

- Provisions for salvage, cleanup, and rebuilding of the primary site are included in the COOP plan.

☐ **Recovery *equipment and supplies* have been identified.**

- All computing recovery requirements (e.g., number of servers, space on servers, memory on servers) have been determined and are documented in the IT/DR Plan.
- All necessary support equipment (e.g., copy machines, fax machines, etc.) needed for recovery has been determined and documented in and arrangements to obtain the equipment are detailed in the COOP plan.
- All special forms and supplies needed for recovery and reconstitiution are identified in and arrangements to obtain them are documented in the COOP plan.
- All voice and data communications equipment needed (e.g., switches, multiplexors) to support the critical business processes are identified in and backup provisions for this equipment are detailed in the COOP plan.
- Back-ups are run nightly, media tapes are stored off-site, and labeled for easy retrieval; data replication is tested for recovery usage and intergrity.

☐ **Emergency *contact lists* have been made available.**

- A list of all employees to be involved in the recovery effort, with their office and home phone numbers, is included in the COOP plan.
- All vendor/supplier names and phone numbers that support the critcial business processes are included in the COOP plan.
- A plan distribution list is included in the COOP plan.
- Team notification procedures (e.g., phone trees, emergency notification systems) are included in the COOP plan.

☐ **Plan *testing* is taking place.**

- Scheduled tests of the COOP plan are performed.
- Detailed test plans, including test objectives, scope, and timing exist for every test performed.
- All test results and plan deficiencies are documented during and after the test of the COOP plan.
- The COOP plan and/or its supporting appendices are tested on a regular and frequent basis (at least one time per year).

☐ **Plan *maintenance* is being performed.**

- COOP plan versions are numbered to avoid accidental use of an old plan.
- Documented procedures exist to keep the COOP plan current following changes made to the agency (e.g., new systems, organizational changes).
- Responsibility for the maintenance of the COOP plan is assigned to a specific individual;
- COOP plan documents are maintained both on-site and off-site.
- COOP plans are updated every April.

C. Terms and Definitions

Term	Definition
Activation	Once a COOP plan has been put into action during a real-life event, whether in whole or in part, it is considered "activated."
After-Action Report (AAR)	A document that reports a chronological timeline and observations of the incident and makes recommendations for post-incident improvement planning.
Agency	Any agency, department, board, or commission in the State of Ohio government
Agency Business Continuity Coordinators	Representatives of each State agency tasked with coordinating the agency's COOP program.
Agency Leadership	The highest-ranking official of the agency, or a successor or designee who has been selected by that official. The designation as a successor enables an individual to act on behalf of leadership and exercise the powers and authorities of the official's position, in the event of the official's death, disability, or resignation.
Agency Mission Essential Function (MEF)	The limited set of agency-level mission essential functions that must be continued throughout, or resumed rapidly after, a disruption of normal activities.
All-hazards	The spectrum of all types of hazards including accidents, technological events, natural disasters, terrorist attacks, warfare, and chemical, biological including pandemic influenza, radiological, nuclear, or explosive events.
Alternate Work Location (AWL)	Locations, other than the primary facility, used to carry out essential functions by relocating employees following activation of the continuity plan. Refers to not only other facilities and locations, but also work arrangements such as telework and mobile work concepts.
Business Continuity (BC)	An enterprise approach which ensures that all State agencies, departments, boards, and commissions will have a viable COOP program and COG capabilities in place. This combined planning effort (COOP+COG) is referred to as business continuity.
Business Impact Analysis (BIA)	A method of identifying the effects of failing to perform a function or requirement.
Business Process Analysis (BPA)	A method of examining, identifying, and mapping the functional processes, workflows, activities, personnel expertise, systems, data, and facilities inherent in the execution of a function or requirement.
Communications	Voice, video, and data capabilities that enable an agency's leadership and staff to conduct the mission essential functions of the agency. Robust communications help ensure that leadership receives coordinated, integrated policy and operational advice and recommendations and will provide the ability for governments and the private sector to communicate internally and with other entities (including with other Federal, State, and Local agencies; the private sector; and citizens) as necessary to perform their mission essential functions.
Continuity	An uninterrupted ability to provide services and support, while maintaining organizational viability, before, during, and after an event.
Continuity Capability	The ability of an agency to continue to perform its mission essential functions, using State-identified Business Continuity programs and continuity requirements that have been integrated into the agency's daily operations, with the primary goal of ensuring the preservation of government and the continuing performance of SEFs under all conditions. Building upon a foundation of continuity planning and continuity program management, the pillars of a continuity capability are leadership, staff, communications, and facilities.

Continuity Communications	Communications that provide the capability to perform essential functions, in conjunction with other organizations until normal operations can be resumed.
Continuity of Government (COG)	A coordinated effort within the State of Ohio to ensure that the SEFs continue to be performed during any interruption to business.
Continuity of Operations (COOP)	An effort within individual agencies to ensure they can continue to perform their MEFs and PMEFs during a wide range of events, including localized acts of nature, accidents, and technological or attack-related incidents.
Continuity Program Management Cycle	An ongoing, cyclical model of planning, training, evaluating, and implementing corrective actions for continuity capabilities.
Corrective Action Plan (CAP)	A plan written after an AAR that allows agencies to analyze, plan for, document, and implement improvements in their continuity plans and programs.
Critical Infrastructure	An interdependent network of vital physical and information facilities, networks, and assets, including telecommunications, energy, financial services, water, and transportation sectors, that private business and the Government rely upon. Critical infrastructures are those systems and assets so vital that their incapacity or destruction would have a debilitating impact on the security of the State and/or the public health and/or safety of citizens.
Critical Infrastructure Protection (CIP)	Risk management actions intended to prevent a threat or threat agent from attempting to, or succeeding at, destroying or incapacitating critical infrastructures.
Delegations of Authority	Identification, by position, of the authorities for making policy determinations and decisions at all agency locations (e.g., HQ, field offices, satellite offices, etc.). Generally, pre-determined delegations of authority will take effect when normal channels of direction have been disrupted and will lapse when these channels have been reestablished.
Devolution	The capability to transfer statutory authority and responsibility for MEFs from an agency's primary operating staff and facilities to other employees and facilities, and to sustain that operational capability for an extended period of time.
Disaster Recovery Institute International (DRII)	A non-profit, internationally known organization that helps organizations spanning private and public sector prepare for and recover from disasters through thoughtful leadership, education, and accreditation.
Emergency Operations Center (EOC)	The physical location at which the coordination of information and resources to support incident management activities normally takes place. An EOC may be a temporary facility or may be located in a more central or permanently established facility.
Emergency Operations Plan (EOP)	A plan for responding to specific hazards (e.g., dam failure, flooding, wild fire, etc.). For the State of Ohio, the EOP is managed by the Ohio Department of Public Safety, Emergency Management Agency (EMA) and supported by 12 other State agencies.
Emergency Operating Records	Records that support the execution of an agency's essential functions.
Emergency Relocation Group (ERG)	Pre-designated staff that move to a relocation site to continue essential functions in the event that their normal work locations are threatened or have been incapacitated by an incident. The ERG is composed of an advance team plus emergency personnel.
Emergency Relocation Group (ERG) Member	A person who has been assigned responsibility to report to an alternate site, as required, to perform mission essential functions or other tasks related to continuity of operations.
Emergency Relocation Group (ERG) Member Planning Guide	Provides tools for developing ERG positional standard operating procedures to support continuity programs. ERG positional guides assist staff in understanding the key elements of performance in that position and allow business continuity coordinators access to positional requirements considered

	when preparing a business impact analysis of the agency's mission essential functions.
Essential Databases	Information systems that are needed to support essential functions during a continuity situation.
Essential Records	Electronic and hardcopy documents, references, databases, and records that are needed to support mission essential functions during a continuity situation. The two basic categories of essential records are (1) emergency operating records and (2) rights and interests records.
Essential Records Packet	A checklist that assists with the identification of, protection of, and readies availability of an agency's essential records.
Essential Resource	Resource(s) that support the organization's ability to provide vital services, exercise civil authority, maintain the safety and well-being of the general populace, and sustain the Nation's industrial and economic bases during an emergency.
Exercise Appendices	A series of documents for agency's to follow in developing exercises that are compatible with the Homeland Security Exercise and Evaluation Program (HSEEP), meeting National Exercise Program requirements.
Facility(ies)	Locations where an organization's leadership and staff operate. Leadership and staff may be co-located in one facility or dispersed across many locations and connected by communications systems. Facilities should be able to provide staff with survivable protection and should enable continued and endurable operations.
Facility Degradation Appendix	Provides a structured action plan, listing steps taken by specific members of facility response teams in the event of a degraded facility.
Federal Emergency Management Agency (FEMA)	FEMA is an agency within the United States Department of Homeland Security, responsible for coordinating the response to a disaster that has occurred in the United States and has overwhelmed the resources of local and state authorities. The Governor must declare a state of emergency and formally request assistance from FEMA before the federal government may respond.
Full-scale Exercise	The most comprehensive type of test that may be performed by an agency. In this type of exercise, the agency implements all or portions of its COOP Plan by processing data and transactions using back-up media at an alternate recovery site, typically under simulated operating conditions.
Functional Exercise	Involves the actual mobilization of personnel to other sites in an attempt to establish communications and coordination as set forth in the COOP Plan. This type of exercise is conducted on one or more components of the COOP Plan under actual operating conditions.
Hazard	Something potentially dangerous or harmful, often the root cause of an unwanted outcome
U.S. Department of Health and Human Services (HHS)	HHS is a federal agency that works to improve the health and well-being of all Americans. HHS's mission is to protect all American by providing essential human services to the public, and advancing the science underlying medicine, public health, and social services.
Homeland Security Exercise and Evaluation Program (HSEEP)	A capabilities-based and performance-based program that furnishes standardized policies, doctrines, and terminologies for the design, development, performance, and evaluation of homeland security exercises. The NEP uses the HSEEP as a common methodology for exercises. The HSEEP also provides tools and resources to facilitate the management of self-sustaining homeland security exercise programs.
Hot Site	An AWL that already has in place the computer, telecommunications, and environmental infrastructure required to recover critical business functions or information systems.

Improvement Plan (IP)	A cycle of events that incorporates evaluations, after-action reports, and lessons learned into the development and implementation of a document (the improvement plan itself) that identifies specific corrective actions, assigns them to responsible parties, and establishes targets for their completion.
Incident	An occurrence or event, natural or man-made, which requires an emergency response to protect life or property. Incidents can, include major natural disasters, critical events, terrorist attacks, terrorist threats, wild and/or urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response.
Incident Action Plan (IAP)	A written plan containing general objectives reflecting the overall strategy for managing an incident. The IAP may include the identification of operational resources and assignments and attachments that provide direction and important information for management of the incident during one or more operational periods.
Initial Response	Resources initially committed to an incident.
Interagency Agreements	A written agreement entered into between agencies that require specific goods or services to be furnished or tasks to be accomplished by one agency in support of the other.
Interoperability	"Interoperability" has two meanings: (1) The ability of systems, personnel, or agencies to provide services to and accept services from other systems, personnel, or agencies, and to use the services so exchanged so that these organizations can operate together effectively; (2) A condition that is realized among electronic-communications operating systems or grids and/or among individual electronic-communications devices, when those systems and/or devices allow the direct, seamless, and satisfactory exchange of information and services between the users of those systems and devices.
IT Disaster Recovery Plan Appendices	Apply to major, usually catastrophic, incidents that deny access to the normal computer center for an extended period. The IT Disaster Recovery Plan(s) may also refer to a systems-focused plan designed to restore operability of the target systems, applications, and/or computer facility at an alternate site after a disaster. Per the NIST Standard Procedure (SP) 800-53, the State of Ohio plans for IT Disaster Recovery based on the criticality or the impact of the system: low, moderate, or high.
Legal and Financial Records	Records that are necessary to protect the legal and financial rights of both the government and private sector and the persons who are affected by its actions.
Memorandum of Understanding (MOU)	A non-binding agreement between two or more parties that outlines how they will work together. MOUs are also known as letters of intent (LOI) or letters of agreement (LOA)
Mission-critical Data	Information that is essential to supporting the execution of an agency's mission essential functions.
Mitigation	Multiagency coordination systems provide the architecture to support coordination for incident prioritization, critical resource allocation, communications systems integration, and information coordination. The components of multiagency coordination systems include facilities, equipment, emergency operations centers (EOCs), specific multiagency coordination entities, personnel, procedures, and communications. These systems assist agencies and organizations to fully integrate the subsystems of the NIMS.
Multi-Year Strategy and Program Management Plan (MYSPMP)	A process that ensures the maintenance and continued viability of COOP plans. The MYSPMP sserves as a roadmap for agency BC coordinators to follow to ensure that critical activities and resources can be implemented and obtained so that the agency's programs continue to improve over time. The MYSPMP

	provides strategic guidance, a current program assessment, and outlines program needs, goals, objectives, and strategies for the agency's COOP as well as milestones for accomplishing these activities and any issues, concerns, or obstacles that they may face.
Mutual-Aid Agreement (MAA)	A a non-contractual agreement between two or more parties to provide assistance to each other during an emergency. MAAs can be used by agencies, organizations, and jurisdictions to provide a legal basis for sharing resources, facilitate the rapid deployment of emergency support, and/or to protect the public's health. MAAs can be established before, during, or after an incident. MAAs can also authorize the sharing of personnel, equipment, supplies, facilities, and other services. The agreements are generally between neighboring communities, states, and/or federal agencies.
National Incident Management System (NIMS)	A system mandated by HSPD-5 that provides a consistent nationwide approach for Federal, State, local, and tribal governments; the private sector; and nongovernmental organizations to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. To provide for interoperability and compatibility among Federal, State, local, and tribal capabilities, the NIMS includes a core set of concepts, principles, and terminology. HSPD-5 identifies these as the ICS; multiagency coordination systems; training; identification and management of resources (including systems for classifying types of resources); qualification and certification; and the collection, tracking, and reporting of incident information and incident resources.
National Institute of Standards and Technology (NIST)	NIST is an agency within the United States Department of Commerce responsible for promoting innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.
Normal Operations	The broad functions that are undertaken by an agency when it is assigned responsibility for a given functional area. These functions include planning and execution of tasks through the full range of agency business services.
Orders of Succession	Provisions that identify and determine succession of staff that will take command during and/or after an incident, if agency leadership is incapacitated or unavailable. Pre-establishing this chain of command enables an orderly transition of leadership, while also ensuring that respective successors are able to be cross-trained on duties in advance.
Ohio Emergency Management Agency (EMA)	Ohio EMA is a division of the Ohio Department of Public Safety, responsible for coordinating the response to a disaster that has occurred in the State of Ohio that has overwhelmed the resources of local authorities.
Pandemic	An epidemic of infectious disease that has a sudden increase in cases and spreads across a large range of continents or worldwide, affecting a substantial number of individuals. Widespread endemic diseases with a stable number of infected individuals such as recurrences of seasonal influenza are generally excluded as they occur simultaneously in large regions of the globe rather than being spread worldwide.
Pandemic Appendix	Provides guidance to an agency in responding to a pandemic, including general guidance and sample information for reference.
Plan	A proposed or intended method of getting from one set of circumstances to another. A plan is often used to move from the present situation towards the achievement of one or more objectives or goals.
Preparedness	The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents. Preparedness is a continuous process. Preparedness involves efforts at all levels of government and between

	government and private-sector and nongovernmental organizations to identify threats, determine vulnerabilities, and identify required resources. Within the NIMS, preparedness is operationally focused on establishing guidelines, protocols, and standards for planning, training and exercises, personnel qualification and certification, equipment certification, and publication management.
Prevention	Actions to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and, as appropriate, specific law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity and apprehending potential perpetrators and bringing them to justice.
Program	A group of related initiatives managed in a coordinated way, so as to obtain a level of control and benefits that would not be possible from the individual management of the initiatives. Programs may include elements of related work outside the scope of the discrete initiatives in the program.
Orders of Succession	Identify and determine succession of personnel staff that will take command during and/or after an incident, if agency leadership is incapacitated or unavailable. Pre-establishing this chain of command enables an orderly transition of leadership, while also ensuring that respective successors are able to be cross-trained on duties in advance.
Reconstitution	The process by which surviving and/or replacement agency personnel resume normal organization operations from the original or replacement primary operating facility.
Reconstitution Appendix	Provides structure and recommended content for developing a reconstitution plan.
Recovery	The implementation of prioritized actions required to return an organization's processes and support functions to operational stability following an interruption or disaster.
Recovery Point Objective (RPO)	How much data the agency is willing to lose should backups be required to return the system or business process to operational status.
Recovery Time Objective (RTO)	The maximum amount of time that a function can be down before the loss in both revenue and data and the cost of resuming the function becomes insurmountable. Depending upon the criticality of the function, the RTO may be immediate resumption or may allow for several days of downtime.
Report-in Location	Location or facilities where incoming resources can check in at the incident.
Resource	Personnel and major items of equipment, supplies, and facilities available or potentially available for assignment to incident operations and for which status is maintained. Resources are described by kind and type and may be used in operational support or supervisory capacities at an incident or at an EOC.
Resource Management	Efficient incident management requires a system for identifying available resources at all jurisdictional levels to enable timely and unimpeded access to resources needed to prepare for, respond to, or recover from an incident. Resource management under the NIMS includes mutual-aid agreements; the use of special Federal, State, local, and tribal teams; and resource mobilization protocols.
Response	Activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations

	plans and of mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.
Risk Analysis	The process by which hazards and risks are identified and evaluated. This is the first step in conducting a risk assessment.
Risk Assessment (RA)	The overall process of identifying, evaluating, and prioritizing risks.
Risk Management	The process of identifying, controlling, and minimizing the impact of risks.
Staff	All personnel who provide the leadership, advice, recommendations, and functional support necessary to continue essential operations.
Standard	A document which either directly supports or provides leading practice guidance through regulations, laws, and generally-accepted practices.
Standard Operating Procedure (SOP)	Complete reference document or an operations manual that provides the purpose, authorities, duration, and details for the preferred method of performing a single function or a number of interrelated functions in a uniform manner.
State Mission Essential Function (SEF)	Statewide Mission Essential Functions – validated by the Business Continuity Steering Committee (BCSC), the Director of the Ohio Department of Administrative Services, and ultimately the Governor of the State of Ohio – which must be performed before during, and after an incident in order to support the continuity of government of the State of Ohio. These SEFs must be continuous or resumed within 12 hours of an incident's occurrence and maintained for up to 30 days or until normal operations can be resumed.
Strike Appendix	A document which provides a structure for management response to a staff shortage or strike scenario.
Structured Walk-through Exercise	Basic test to ensure that critical personnel from all of the COOP sections and appendices are familiar with the Business Continuity Plan, activities, and recovery procedures.
Tabletop Exercise (TTX)	The tabletop is largely a discussion guided by a facilitator (or sometimes two facilitators who share responsibilities). Its purpose is to solve problems as a group. There are no simulators and no attempts to arrange elaborate facilities or communications. One or two evaluators may be selected to observe proceedings and progress toward the objectives.
Telework	The ability to work at a location other than the official duty station, using portable computers, high-speed telecommunications links, and mobile communications devices.
Testing, Training, and Exercise (TT&E) Program	Measures to ensure that an organization's continuity plan is capable of supporting the continued execution of the organization's essential functions throughout the duration of a continuity situation.
Threat	An indication of possible violence, harm, or danger.
Warm Site	An AWL that is equipped with some hardware, and communications interfaces, electrical and environmental conditioning which is capable of providing backup after additional provisioning, software or customization is performed.

D. Record of Changes

Date	Description of Updates	Revised By:
07/09/2014	Initial Draft	Melinda Craig
02/13/2015	Addition of the following sections: • Essential Employee Designation and Policy • Training, Testing, and Exercise • Record Retention • Public Record Classification • Terms and Definitions	Melinda Craig
08/05/2015	Updated BIA process description to reflect change from detailed interview format to simplified heat map	Melinda Craig
08/08/2016	Updated Business Continuity Program contact information	Melinda Craig
07/01/2017	Administrative updates	Melinda Craig
03/30/2018	Updated to align with FEMA Continuity Guidance circular	Melinda Craig
03/01/2019	Administrative updates	Melinda Craig
01/06/2020	Updated pandemic planning recommendations to align with FEMA, HHS, and multi-jurisdictional State working group recommendations	Melinda Craig
02/06/2021	Updates telework planning recommendations based on administrative guidance from the Governor of Ohio and Ohio DAS	Melinda Craig
06/05/2022	Updates to training recommendations, resources, and references based on guidance from FEMA National Continuity Program	Melinda Craig
08/23/2023	Resource and branding updates from Ohio DAS Communications Office	Melinda Craig
03/24/2024	Addition of newly acquired State-owned facility (A.B. Graham) to Risk Assessment Section	Melinda Craig
02/26/2025	Administrative updates	Melinda Craig