Your Logo
Will Be
Placed Here

CONTINUITY OF OPERATIONS PLAN (COOP)

[Official Company Name]

Table of Contents

REFERENCED FRAMEWORKS & SUPPORTING PRACTICES

This document references numerous leading industry frameworks in an effort to provide a holistic approach to designing and maintain processes to ensure the confidentiality, integrity, availability and safety (CIAS) of [Official Company Name] ([Company Name])'s systems, applications, services and data. The following external content is referenced by or supports this Continuity of Operations Plan (COOP):

- The National Institute of Standards and Technology (**NIST**): [1]
  - NIST 800-34: *Contingency Planning Guide for Federal Information Systems*
  - NIST 800-37: *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
  - NIST 800-39: *Managing Cybersecurity Risk: Organization, Mission and Information System View*
  - NIST 800-50: *Building An Information Technology Security Awareness and Training Program*
  - NIST 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations*
  - NIST 800-84: *Guide To Test, Training and Exercise Programs for IT Plans and Capabilities*
  - NIST 800-171: *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*
  - NIST 800-181: *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*
  - NIST IR 7298: *Glossary of Key Cybersecurity Terms*
  - NIST IR 8179: *Criticality Analysis Process Model: Prioritizing Systems and Components* [draft]
  - NIST *Framework for Improving Critical Cybersecurity* (Cybersecurity Framework)
- The International Organization for Standardization (**ISO**):[2]
  - ISO 15288: *Systems and Software Engineering -- System Life Cycle Processes*
  - ISO 22301: *Societal Security – Business Continuity Management Systems – Requirements*
  - ISO 27002: *Information Technology -- Security Techniques -- Code of Practice for Cybersecurity Controls*
- Other Frameworks:
  - Federal Emergency Management Agency Incident Command System (**FEMA ICS**)[3]
  - FEMA Natural Disaster Recovery Framework (**FEMA NDRF**)[4]
  - FEMA National Response Framework (**FEMA NRF**)[5]
  - Cloud Security Alliance Cloud Controls Matrix (**CSA CCM**)[6]
  - Center for Internet Security Critical Security Controls (**CIS CSC**)[7]
  - Control Objectives for Information and Related Technologies (**COBIT**)[8]
  - European Union Regulation 2016/279 (General Data Protection Regulation (**EU GDPR**))[9]

[1] National Institute of Standards and Technology - http://csrc.nist.gov/publications/PubsSPs.html
[2] International Organization for Standardization - https://www.iso.org
[3] Federal Emergency Management Agency - https://training.fema.gov/EMIWeb/IS/ICSResource/index.htm
[4] FEMA NDRF - https://www.fema.gov/national-disaster-recovery-framework
[5] FEMA NRF - https://www.fema.gov/media-library-data/1466014682982-9bcf8245ba4c60c120aa915abe74e15d/National_Response_Framework3rd.pdf
[6] Cloud Security Alliance - https://cloudsecurityalliance.org/
[7] Center for Internet Security - https://www.cisecurity.org/
[8] COBIT - http://www.isaca.org/COBIT/Pages/default.aspx
[9] EU General Data Protection Regulation - http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

CONTINUITY OF OPERATIONS PLAN (COOP) OVERVIEW

INTRODUCTION

The Continuity of Operations Plan (COOP) provides authoritative guidance on the prescribed measures used to establish and maintain Business Continuity and Disaster Recovery (BC/DR) capabilities at [Company Name].

Protecting [Company Name] data and the systems that collect, process and store this information is of critical importance. Consequently, the security of systems must include controls and safeguards to offset possible threats, as well as controls to ensure accountability, availability, integrity, confidentiality and safety of the data:

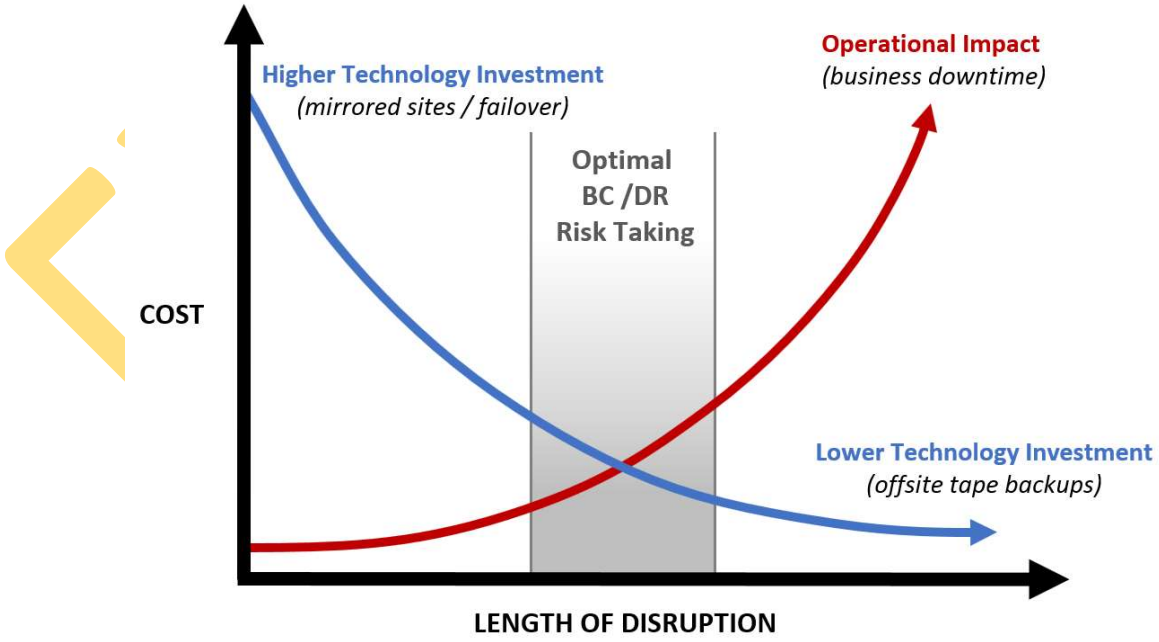
- Confidentiality – Confidentiality addresses preserving restrictions on information access and disclosure so that access is restricted to only authorized users and services.
- Integrity – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- Availability – Availability addresses ensuring timely and reliable access to and use of information.
- Safety – Safety addresses reducing risk associated with embedded technologies that could fail or be manipulated by nefarious actors.

PURPOSE

The purpose of the Continuity of Operations Plan (COOP) is to prescribe a comprehensive framework for:

- Creating a Business Continuity Management System (BCMS);
- Protecting the Confidentiality, Integrity, Availability and Safety (CIAS) of [Company Name]'s systems, applications, services and data;
- Recognizing the highly-networked nature of the current computing environment and provide effective company-wide management and oversight of those related cybersecurity risks; and
- Providing for the development, review and maintenance of security controls required to ensure the continuity of business processes.

Commensurate with assessed risk, security measures must be implemented to provide cost-effective and sustainable ways to protect [Company Name] assets against reasonably-foreseeable natural and man-made disasters.



CONCEPT OF OPERATIONS (CONOPS)

The concept of the Continuity of Operations Plan (COOP) is to establish Business Continuity & Disaster Recovery (BC/DR) processes that will enable [Company Name] to recover from adverse situations with a minimal negative impact on operations.

CONTINUITY OF OPERATIONS PLAN (COOP) FRAMEWORK

The COOP takes a holistic approach to BC/DR that utilizes a phased approach to preparing for and responding to incidents.

PHASE 1 PREPARE	PHASE 2 REACT	PHASE 3 RECOVER	PHASE 4 TRANSITION	PHASE 5 REVIEW & IMPROVE

- Phase 1 – Prepare
- Phase 2 – React
- Phase 3 – Recover
- Phase 4 – Transition
- Phase 5 – Review & Improve

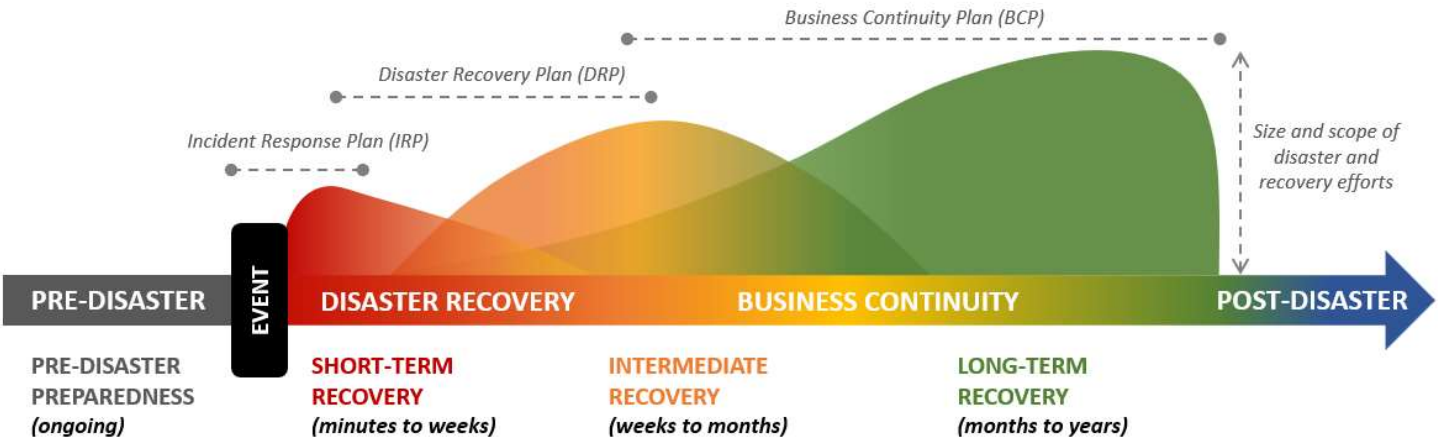
This phased approach incorporates several different incident response and BC/DR components to create a centralized and strategic approach to emergency management that can scale to deal with the size and scope of disasters and recovery efforts.

These phases overlap from incident response at a tactical level (IRPs and DRPs) to intermediate and long-term recovery efforts at a strategic level (BCPs):

- Incident Response Plans (IRPs)
- Disaster Recovery Plans (DRPs)
- Business Continuity Plans (BCPs)

It is important to keep in mind that most disasters start off with incident response that require IRPs. As events escalate, DRPs are activated and then transition into BCPs. The COOP covers this spectrum of response, but there are important distinctions:

- Disaster Recovery (DR) is data-centric.
- Business Continuity (BC) is business-centric.



COOP Strategy

[Company Name]'s business continuity strategy is to cost-effectively manage BC/DR risks through the development, implementation and governance of processes and documentation to facilitate the implementation of an enterprise-wide Continuity of Operations Plan (COOP) that is supported through associated policies, standards, controls and procedures.

COOP Mission

To ensure the appropriate People, Processes and Technology (PPT) exist, are properly prepared, and are able to execute BC/DR operations in less-than-optimal conditions with little or no advanced notice.

Operational Locations

The following physical locations are within scope for [Company Name]'s COOP:

World Headquarters (WHQ)

[insert physical address here]
[insert COOP Point of Contact (POC) & contact information here]

Primary Processing Site (PPS)

[insert physical address here]
[insert COOP Point of Contact (POC) & contact information here]

Alternate Processing Site (APS)

[insert physical address here]
[insert COOP Point of Contact (POC) & contact information here]

Primary Storage Site (PSS)

[insert physical address here]
[insert COOP Point of Contact (POC) & contact information here]

Alternate Storage Site (ASS)

[insert physical address here]
[insert COOP Point of Contact (POC) & contact information here]

Other Operational Locations

[insert physical address here]
[insert COOP Point of Contact (POC) & contact information here]

Operational Requirements

BC/DR professionals rely on well-known metrics that are used to drive planning of emergency operations procedures and continuity of operations procedures. These metrics are:

Capability Resilience Level (CRL)

A CRL is the relative degree to which a capability can be impacted by a single disaster event. [Company Name]'s target CRL is [insert # from the table below that reflects the appropriate CRL].

CRL	Description
1	One (1) production site with onsite storage.
2	One (1) production site with offsite storage.
3	One (1) production site with cloud-based processing and storage.
4	Two (2) production sites in close proximity with localized processing and storage.
5	Two (2) production sites in close proximity with cloud-based processing and storage.
6	Three (3) or more geographically-dispersed production sites with localized processing and storage.
7	Three (3) or more geographically-dispersed production sites with cloud-based processing and storage.

Maximum Tolerable Downtime (MTD)

The MTD is a time value that represents the greatest period of time that [Company Name] is able to tolerate the outage of a critical process or system without sustaining permanent damage to the organization's ongoing viability. [Company Name]'s stated MTD for key business functions are:

MTD Target (s/m/h/d/w/m)	Function	Description
[example] 3 days	Email communications	Corporate email
x		
x		
x		
x		
x		

Recovery Point Objective (RPO)

The RPO is a time value that describes the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds [Company Name]'s maximum allowable threshold. RPO is largely dependent on backup processes to write data locally or replicate data to another location. [Company Name]'s stated RPOs are:

RPO Target (s/m/h/d/w/m)	Function	Description
[example] 8 hours	Database X	Employee Resource Management (ERM) database
x		
x		
x		
x		
x		

PHASE 1 – PREPARE

PHASE 1 PREPARE	PHASE 2 REACT	PHASE 3 RECOVER	PHASE 4 TRANSITION	PHASE 5 REVIEW & IMPROVE

This phase addresses the preparation aspect of the COOP, since a failure to plan is tantamount to a plan to fail.

MISSION ESSENTIAL FUNCTIONS (MEF)

As part of [Company Name]'s annual risk management activities, it is important to identify Mission Essential Functions (MEFs) through a Business Impact Analysis (BIA) to rank applications, services, systems, supporting infrastructure and third-party services into an appropriate MEF categorization.

Safety & Criticality Classification	MEF Tier	Recovery Function Priority Description	Recovery Time Objective (RTO)
SC-1 Mission Critical	1	MEF Tier 1 functions involve those with the *direct and immediate effect* on the organization.	<10 seconds
	2	MEF Tier 2 functions can be delayed until Tier 1 functions are restored but must be operational within twenty-four (24) hours.	<24 hours
SC-2 Business Critical	3	MEF Tier 3 functions can be delayed until Tier 1 and 2 functions are established but must be operational within one week.	24 hours to 1 week
SC-3 Non-Critical	4	MEF Tier 4 functions can be delayed until Tiers 1, 2 and 3 are operational.	1 week to 30 days

Appendix A (Baseline Security Categorization Guidelines) provides guidance on categorizing systems for criticality.

BUSINESS IMPACT ANALYSIS (BIA)

Results of the latest BIA can be viewed at the following network share: [insert location of BIA].

Appendix B (MEF Recovery Prioritization) provides a tiered list of assets, based on recovery prioritization.

These three (3) typical steps are typically involved in accomplishing the BIA:

1) Determining mission/business processes and recovery criticality.
    a. Mission/business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime.
    b. The downtime should reflect the maximum time that [Company Name] can tolerate while still maintaining the mission.
2) Identifying resource requirements.
    a. Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible.
    b. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.
3) Identifying recovery priorities for system resources.
    a. Based upon the results from the previous activities, system resources can be linked more clearly to critical mission/business processes and functions.
    b. Priority levels can be established for sequencing recovery activities and resources.

Capability Development

Preparedness for BC/DR incidents requires a blend of People, Processes and Technology (PPT).

People

Staff listed within the Key Staff Roles must have the appropriate Knowledge, Skills, and Abilities (KSAs) to perform their assigned duties. To ensure KSA are current, these individuals requires annual capability development that at a minimum includes:

- Participating in at least one (1) simulated exercise (e.g., tabletop exercise, failover exercise, etc.); and
- Reading the COOP to maintain familiarity with the content and their expected roles.

Emergency Contact Lists

The BCT Leader is responsible for managing the process of maintaining the accuracy of emergency contact lists to support the COOP:

- At least on an annual basis, the BCT Leader is required to work with stakeholders to ensure the names and contact information of key individuals are verified and updated, as necessary, to accommodate changes in People, Processes and Technology (PPT); and
- The COOP will be updated to reflect the changes in contact information.

Training

Members of the BCT are expected to take the Federal Emergency Management Agency (FEMA) Introduction to Incident Command System (ICS-100) course.[12]

On an annual basis, [Company Name] will conduct at least one scenario-based exercise, which may be a tabletop discussion or a full live exercise. It is imperative that members of the following teams perform an annual review of the COOP, prior to the exercise:

- Senior Management;
- Integrated Security Incident Response Team (ISIRT);
- Business Continuity Team (BCT);
- Damage Assessment Team (DAT);
- Infrastructure Team;
- End User Computing (EUC) Team; and
- Procurement Team.

Processes

The BCT Leader is responsible for managing the process of maintaining the accuracy of systems, applications and processes that are needed for the successful execution of the COOP.

Inventory of Critical Processes

At least on an annual basis, the BCT Leader is required to work with stakeholders to ensure any new or modified processes that impact the COOP are identified and documented. The COOP will be updated to reflect the changes in processes.

Critical Records & Files

At least on an annual basis, the BCT Leader is required to work with stakeholders to ensure any new or modified critical records or files that impact the COOP are identified and documented.

Appendix C (Critical Records & Files) a directory and location of critical records and files that are important for the COOP.

Technology

The BCT Leader is responsible for managing the process of maintaining the accuracy of systems, applications and services that are needed for the successful execution of the COOP.

Inventory of Critical Systems & Applications

At least on an annual basis, the BCT Leader is required to work with stakeholders to ensure any new or modified technologies that impact the COOP are identified and documented.

Appendix B (MEF Recovery Prioritization) provides a tiered list of systems, applications and processes, based on recovery prioritization.

[12] FEMA Emergency Management Institute - https://training.fema.gov/nims/