Continuity of Operations Plan (COOP) in a Cyber Incident

Chris Corwin

Disaster Services Coordinator for Blaine County

Idaho Emergency Managers Association President

What is a COOP?

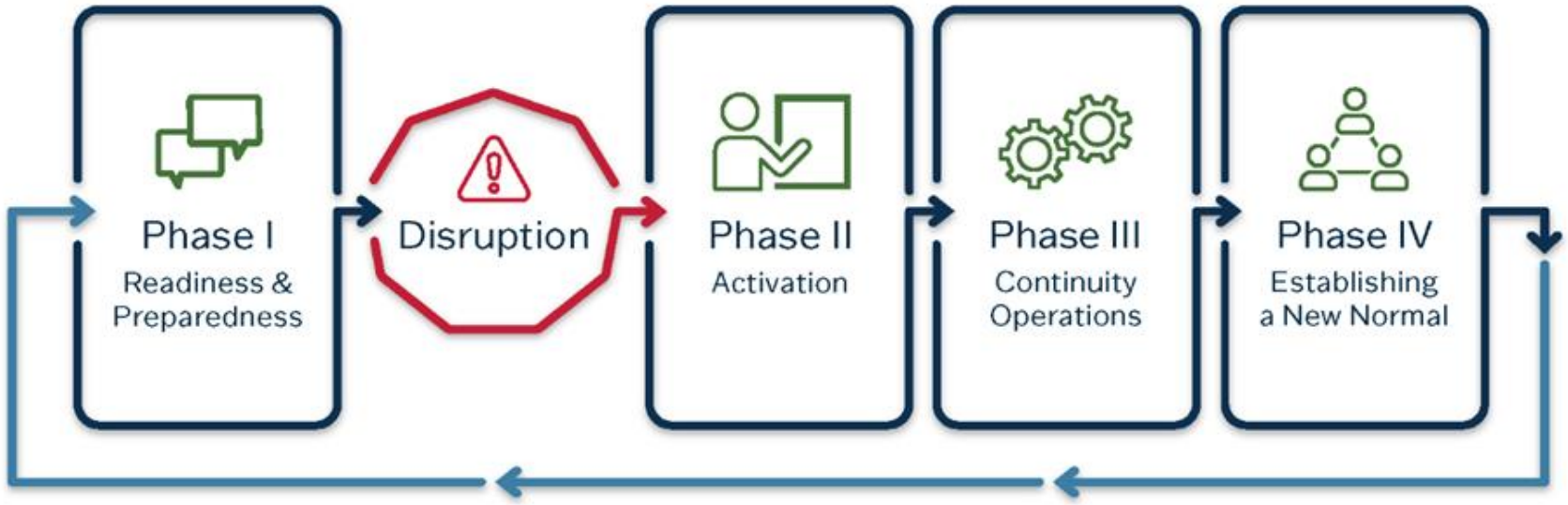
A plan for the uninterrupted performance of essential functions before, during and after events that disrupt normal operations.

It is required of all federal executive departments and agencies

It’s considered a “Best Practice” for State, Local Territorial and Tribal governments.

It’s a coordinated effort within all county services to ensure that essential functions continue to be performed before, during, and after an emergency or threat.

Phases of Continuity:



Step 1: Establish a Planning Team

- Head or Director of Essential Functions
- IT
- Human Resources
- Facilities
- Clerk/Comptroller
- Emergency Management
- Legal

Step 2: Defining Essential Functions

Essential functions are a subset of organizational functions that are critical activities.

In most organizations, not all functions performed on a daily basis are essential.

Identifying essential functions helps an organization determine where to focus their limited time and resources, such as personnel and supplies, during an emergency.

Essential Functions Are:

- Urgent
- Important
- Cannot be deferred

National Essential Functions and How they transfer to SLTT

- NEF1 – Ensure the continued functioning form of government
  - succession to key offices, such as elected officials; communications within the branches of government, government agencies, and the public; leadership and management operations; situational awareness; and personnel accountability.
- NEF2 – Provide visible leadership to maintain trust and confidence.
  - Essential functions can include monitoring threats and hazards and maintaining the confidence of established government organizations and the public.

National Essential Functions and How they transfer to SLTT - Continued

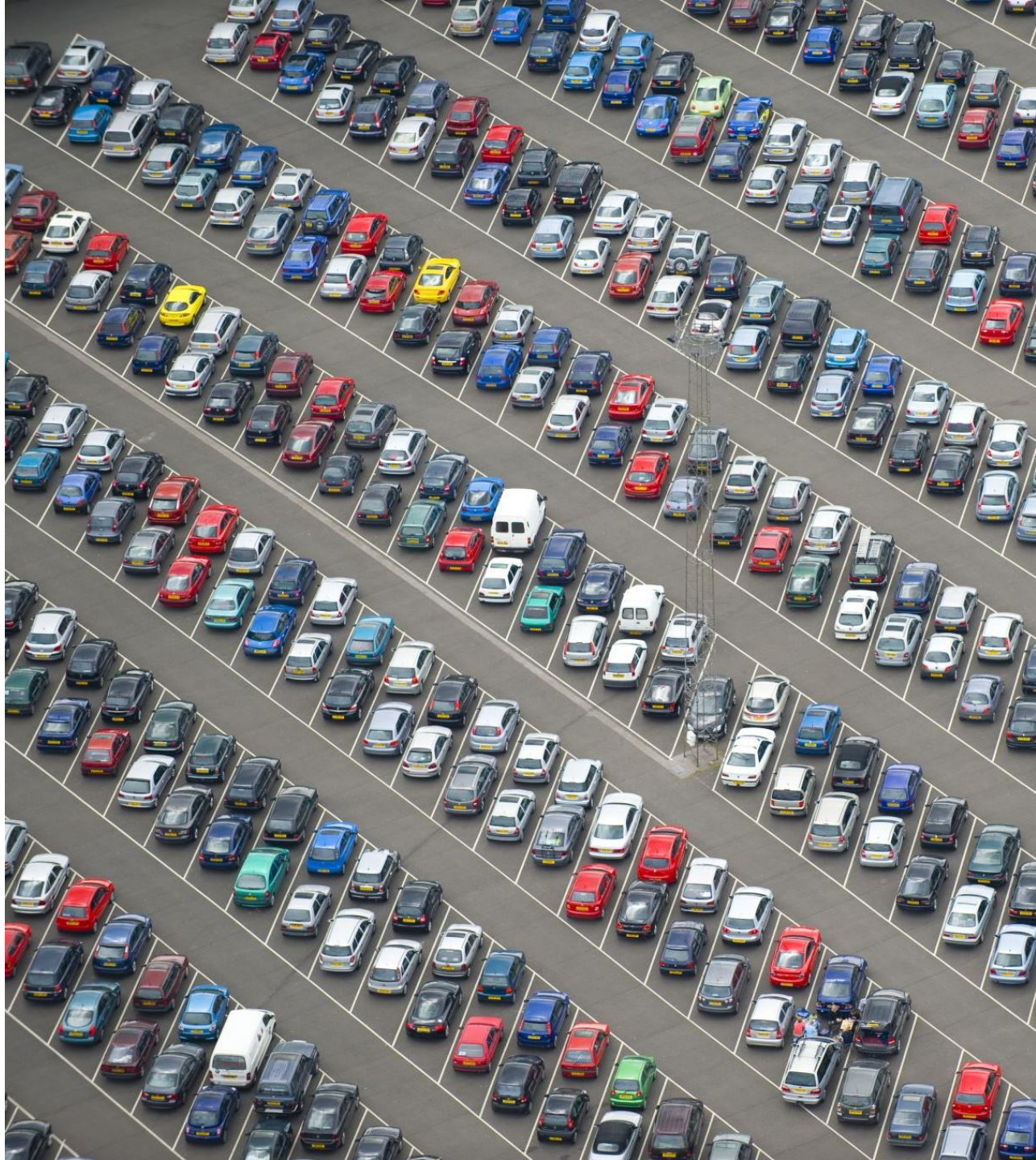
- NEF 3 – Defend the United States
  - Does not translate to local government, other than to help maintain situational awareness and critical infrastructure – communications
- NEF 4 – Maintain and Foster effective relationships
  - Maintain relationships and agreements with federal, state and local partners.
  - Also work with private sector, and non-profit organizations
- NEF 5 – Maintain Law and Order
  - Self explanatory

National Essential Functions and How they transfer to SLTT - Continued

- NEF 6 – Provide Emergency Services
- NEF 7 – Maintain economic stability
  - SLTT governments have a responsibility to manage their jurisdiction's finances, ensure solvency, and ensure that banks, credit unions, savings and loans, and stock and commodity exchanges can open and transact business in accordance with legal obligations, including any power and data services required for transactions.
- NEF 8 – Provide for federal government services that address the national health and welfare needs of the US.
  - Provide basic essential services, focusing on providing water, power, healthcare (including disability services), personal assistance services, communications, transportation services, sanitation services, environmental protection, commerce, education, and childcare.

Example: DMV

- Which if these functions would you say are Essential?
  - Issuing State ID card and driver licenses
  - Issuing of vehicle titles and registrations
  - Providing license plates
  - Performing driver exams
  - Providing safety training
  - Collecting fees



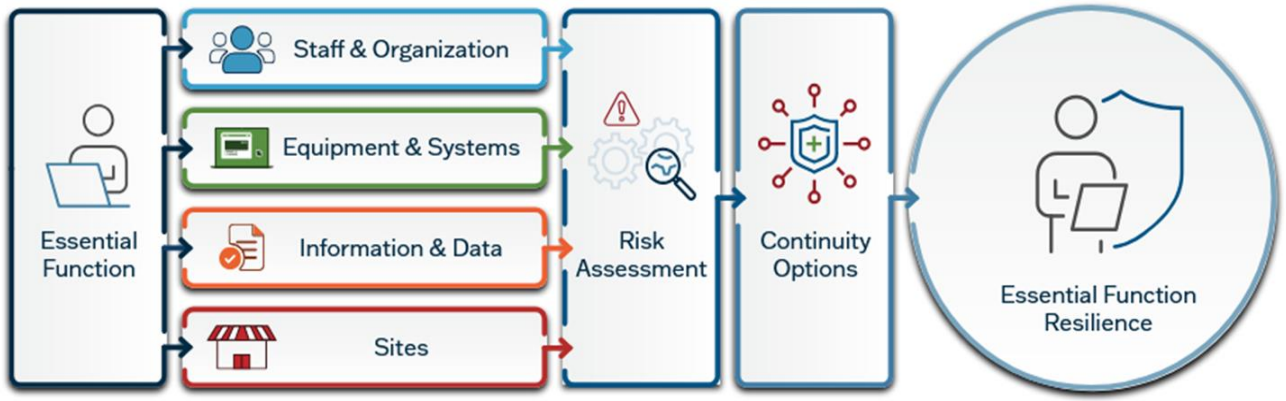
Answer:

- Providing Identification and Driver's Licenses are an essential function for the DMV.
  - These are required for an individual to receive many services in day-to-day life. In an emergency, these identification cards are necessary to receive many forms of assistance.
- As an example, in the case of a wildfire;
  - People would leave behind normal day-to-day items such as wallets, keys, phones, money, and even important papers.
  - Survivors will need a form of identification to qualify for most emergency relief programs and assistance, or potentially to re-enter the impacted area.
- The DMV can defer some day-to-day organizational functions to reallocate resources to issue new identifications, which is a DMV essential function.
- By reallocating personnel and using an alternate facility, the DMV is still able to assist residents until normal operations can be resumed.
- By being prepared early, the DMV can still accomplish the essential function of providing identification to the people.

Should you plan for non-essential functions?

Step 3: Determine How To Do those Functions in the case of a disaster/cyber event

- What are your redundancies?
- If no software for recording, How are you going to record? Do you have SOP? Resources, paper back ups?
- Designated staff may operate from different locations such as an alternate site or telework.
- Some staff may have different assignments, shifts, rotations, or schedules.
- MOUs for use of other Office space.



Staff & Organization

- Personnel rosters.
- Devolution.
- Orders of succession.
- Delegations of authority.
- Personnel preparedness.
- Training.
- Geographically distributed personnel.

Equipment & Systems

- Redundancy (backup power; disaster recovery; Primary, Alternate, Contingency and Emergency [PACE] communications options).
- Systems hardening (e.g., for solar weather).
- Assessments of risks from manufacturers and developers in the equipment and systems supply chain.
- Reserve equipment and backup system inventory.

Information & Data

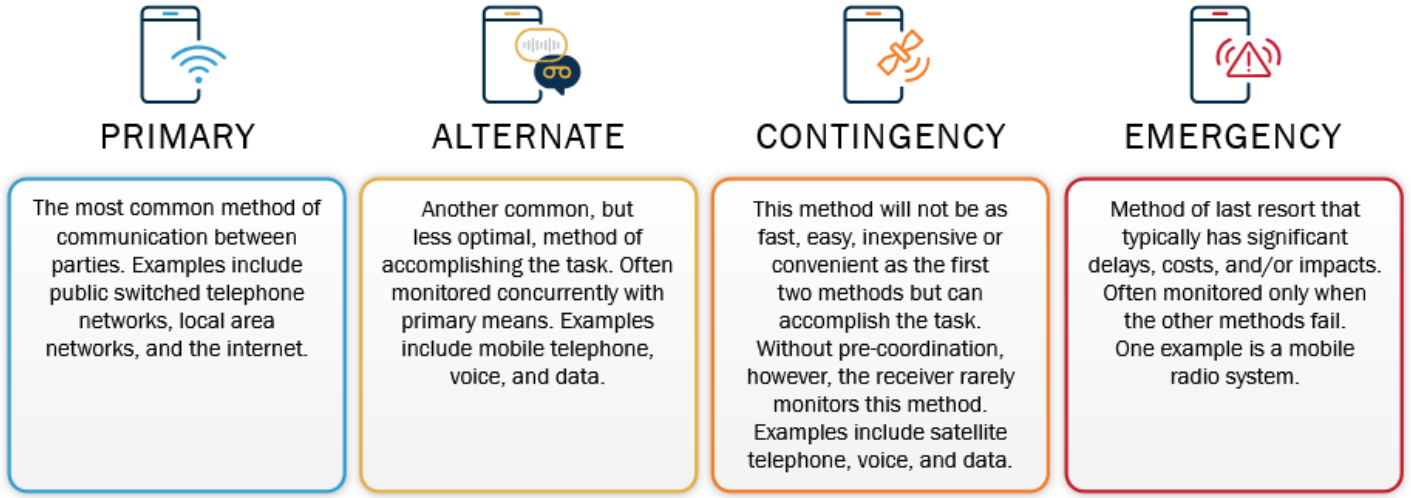
- Printed versions of digital records.
- Digital record backups to alternative servers on external networks.
- Digital records backed up on digital media storage equipment secured in physical locations.
- Data management processes and procedures.
- Cybersecurity.

Sites

- Site redundancy (e.g., alternate operating sites).
- Site distribution (including telework and use of a distributed network of fixed sites).
- Mobile operating sites.
- Alternate water sources.
- Devolution sites.
- Physical security measures at primary and alternate sites.

Step 4: Develop a communications plan

- If no email, how are you going to communicate?
- If no phone?
- What happens if you cannot reach a director of a department? What if you can’t reach a quorum of elected officials?



Step 5: Put it all together

Incident Action Plan

Incident Response Plan

Details:

- Who is in charge
- How you will communicate
- Where you will do the work
- What are your essential functions and how will you complete them in the case of the disruption.
- Plan for returning to normal

Step 6: Exercise or Practice your plan!

- This includes organization-wide continuity readiness and preparedness activities, for example:
  - Plan review, and revision focused on impacts from relevant threats and hazards.
  - Risk management activities. Mitigation.
  - Maintaining training and exercise programs.
  - Reviewing lessons learned and best practices.
- Despite its clear importance, many organizations still treat the COOP as a one-time task. A static plan quickly becomes outdated.

Activation

Assessing potential or realized event impacts.

Activating continuity plans fully or partially.

Moving personnel.

Distributing notifications and internal and external messaging.

Testing contingency capabilities.

Submitting any required status reports

Continuity Operations

- Accounting for personnel.
- Performing essential functions though contingency capabilities.
- Coordinating and collaborating.
- Establishing communications with interdependent organizations and other internal and external stakeholders.
- Submitting any required status updates.

Reconstitution

Reconstitution is the process by which an organization returns to pre-disruption operations and/or establishes a new normal state of operations.

Upon return to the site or reestablishment of normal operations, the final phase of reconstitution begins. Hot washes are conducted and AARs are developed, by which plans, procedures, checklists, and agreements are adjusted as needed.

Summary

Continuity is a critical part of every organization’s mission and ensures the continuation of essential functions and services during a disruption to normal operations.

Essential functions are urgent, important, cannot be deferred or delayed, and required for the organization's mission.

The continuity of every organization contributes to the resilience of the whole community.

www.fema.gov/sites/default/files/documents/fema_continuity-guidance-circular_082024.pdf