Third-party contract compliance in Public Sector entities

BOB FELDMANN

National Public Sector Audit Leader

Your instructors

Elizabeth Watts

Manager

Risk Consulting
Great Lakes Region

Elizabeth (Liz) is a certified fraud examiner with over eighteen years of professional experience at RSM US. Her career has focused on providing risk advisory and contract compliance consulting services for both public and private sector clients, including designing and reporting on contract compliance investigation procedures for both internal assessments and external third-party audits.

Chris Gums

Manager

Risk Consulting
Southeast Region

Chris is a certified internal auditor with over 5 years of experience at RSM. He has dedicated his career to serving clients in the public sector, providing risk consulting and internal audit services. His focus includes facilities and construction, contract compliance, and contract administration, with a specialization in organizational processes, risks, and controls, and contract compliance for large construction manager at risk ("CMAR") contracts.

Agenda

Min	Topic
5	Introduction and objectives
15	Third-party risk & risk management
15	Contract compliance oversight
15	Internal and third-party contract compliance audits
10	Q&A

Objectives

By the end of this course, you will be able to:

- Describe third-party contract risks relevant to the public sector
- Identify compliance red flags and strategies to evaluate compliance with the terms and conditions of contracts and the importance of contract compliance oversight

The big picture

Third-party risk & risk management

Third-party relationships – who are they?

A third-party relationship is any business arrangement between an organization and another entity, by contract or otherwise.

Examples of third-party relationships	
Vendors	Suppliers
Distributors	Licensees
Customers	Professional service providers
Subcontractors	Service contractors
Contract manufacturers	Business partners
Concessionaires	Resellers
Agents/brokers	Non-contractual parties (e.g., UPS)

Examples of out-sourced activities
IT/cybersecurity services
Construction
Accounting/auditing
Supply chain
Cleaning/maintenance
Inspections
Workers comp administration
Social services programs
Uniforms (i.e. fire, police)
Sports/community complex management
Parking operations

Third-party risk in the Public Sector

While all organizations experience some level of exposure to third-party risks, the unique operating environment of the public sector — with ever-growing levels of stakeholder expectations and external scrutiny — creates conditions in which failing to plan appropriately for these third-party risks has unique consequences, including:

- Operational disruptions/delays in essential services (and potential repercussions for community well-being: healthcare, food services, infrastructure maintenance, etc.)
- Financial loss (cost over-runs or revenue leakage)
- Reputational damage
- Compliance risks (i.e. regulatory issues, liability exposures)
- Cyber/information security risks

These risks stem from errors, vulnerabilities, mismanagement or fraud by the third-party. Third-party risk management (TPRM) involves identifying, assessing, and controlling risks that occur due to interactions with third parties, from initial vendor selection to off-boarding. It's not possible to fully eliminate third-party risks, but ensuring that the appropriate measures, contracts, and oversight are in place can reduce or minimize third-party risks and maintain transparency and accountability in the public sector.

Strategies for limiting third-party risk

Document and follow applicable policies (i.e. how third-party vendors are procured, guidelines around risk management and procurement decisions)

Written policies and/or procedures are intended to ensure accountability and transparency throughout the process.

Set expectations

It is essential to set clear expectations when your organization contracts a third party to deliver services in the public sector. Determine key performance indicators (KPIs) such as strategic, operational, and performance goals and identify the desired outcomes of the contract before entering an agreement with a third party.

Ensure the right oversight

After the expectations for the third party are determined, your organization should ensure it has the appropriate structures in place to oversee the delivery of the outsourced services. Monitor and report on results on a regular basis to track performance and ensure the third party is meeting objectives. You can choose to either renew, update, or terminate the contract after it expires based on whether the third party was able to achieve the desired outcomes.

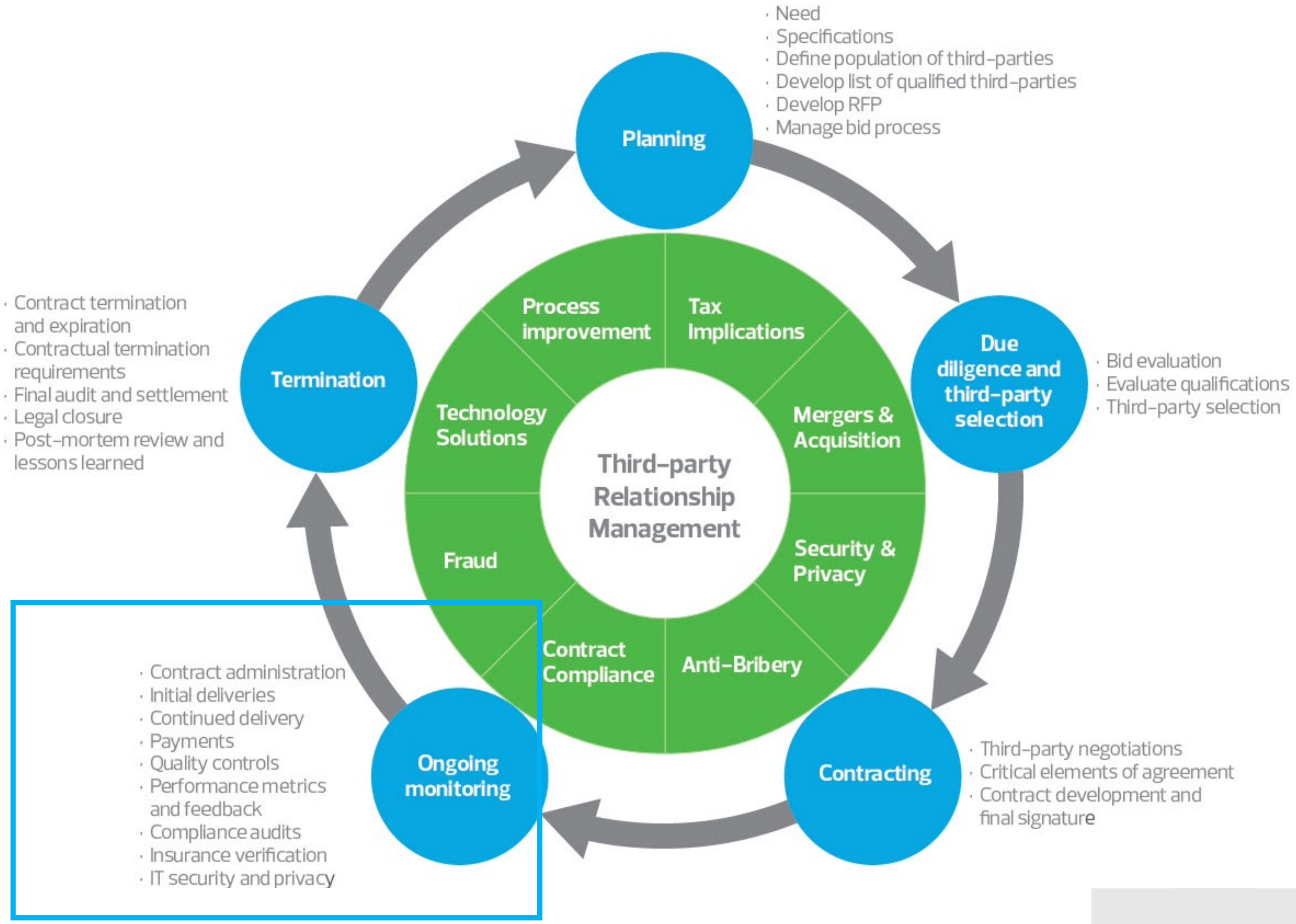
Have a backup plan

Consider contracting multiple vendors to supply the same services. These backups are essential to prevent a delay in services and minimize reputational damage if one vendor does not meet expectations and is released from their contract.

Follow the third-party risk management lifecycle

Keep the third-party risk management lifecycle in mind when outsourcing services to a third party.

Third-party risk management (TPRM) lifecycle



The 3 lines of defense

	First line	Second line	Third line
Roles & Responsibilities	• **Owns the business third-party relationship** and day-to-day oversight of third-party relationship from planning through termination • **Identifies, measures, monitors, controls and reports risks** generated by business third-party relationships • **Implements** a strong risk and control framework and associated policies, procedures, processes and control units to identify, manage and mitigate key risks • Example: **business owners**	• **Designs and owns** the TPRM of system components • **Provides independent, risk-based viewpoint** and guides the first line in risk responsibilities • **Identifies known and emerging risk issues**, as well as shifts in the organization's implicit risk appetite • **Monitors the implementation of effective risk management** practices by the first line • **Independently oversees** aggregate risk exposure; analyzes risk themes and trends, addresses or escalates undesirable risk behaviors • Example: **TPRM group** (i.e., group that oversees day-to-day processes)	• **Independently assesses** adherence to the TPRM components • **Provides assurance** that the TPRM process is functioning as designed • **Identifies improvement opportunities** across TPRM components • Example: **internal audit**
Key Challenges	• Understanding of overall risk exposure to adequately assess the third party, including reputational and strategic risks • Deep understanding of the organization, impacted processes, business units, etc. • Integrating risk management and procurement	• Maintaining independence in the review process • Providing meaningful, valuable challenges to inputs provided by first line • Understanding the overall risk exposure • Minimizing duplicate efforts • Establishing an override protocol between the first and second line	• Minimizing duplicate efforts • Providing risk-based versus coverage-based audit plans to satisfy expanded audit universe and increased regulatory expectations

Contract compliance oversight

Why is contract risk a key consideration?

While all organizations experience some level of exposure to third-party risks, the unique operating environment of the public sector — with ever-growing levels of stakeholder expectations and external scrutiny — creates conditions in which failing to plan appropriately for these third-party risks has unique consequences, including:

- Operational disruptions/delays in essential services (and potential repercussions for community well-being: healthcare, food services, infrastructure maintenance, etc.)
- Financial loss (cost over-runs or revenue leakage)
- Reputational damage
- Compliance risks (i.e. regulatory issues, liability exposures)
- Cyber/information security risks

These risks stem from errors, vulnerabilities, mismanagement or fraud by the third-party. Third-party risk management (TPRM) involves identifying, assessing, and controlling risks that occur due to interactions with third parties, from initial vendor selection to off-boarding. It's not possible to fully eliminate third-party risks, but ensuring that the appropriate measures, contracts, and oversight are in place can reduce or minimize third-party risks and maintain transparency and accountability in the public sector.

Contract compliance oversight

Contract oversight (or administration) involves those activities that begin after the award of a contract. Its purpose is to evaluate whether the vendor (and the organization) is performing in accordance with the terms and conditions of the contract from the time the contract is awarded until the work is complete.

A holistic approach to contract compliance requires, first, an understanding of:

1) the population of your third-party contracts / vendors
2) who in your organization "owns" the responsibility of each contract / vendor
3) the terms and conditions of each contract

… **then** you can build out oversight activities.

Compliance is not a feel-good activity (or a check-the-box exercise).
Compliance drives the bottom line.

Example contract oversight responsibilities

- ✓ Understand the terms and conditions of the contract, including specific requirements that should be enforced.
- ✓ Have regular communication with the vendor and other organization stakeholders to align on scope, contract requirements, and process for work performance and payment
- ✓ Keep relevant parties informed of any technical or contractual challenges, progress of work, and potential problem areas. Document vendor performance issues.
- ✓ Assure timely performance of the contract and verify that performance meets terms of the contract, including schedule, technical specifications, scope of work, and pricing/cost.
- ✓ Invoice review, approval and payment, to include verifying the price/amount charged is correct
- ✓ Verifying vendor is meeting other contractual terms and conditions, such as required reporting, submitting supporting documentation, carrying appropriate insurance, etc.
- ✓ Conduct internal audits to evaluate internal controls related to contract oversight, and/or assess performance and compliance with specific contracts
- ✓ Conduct third-party audits of vendors, in accordance with audit rights of the contract, to assess compliance with specific contracts

Value and benefits of contract oversight

A documented contract oversight process will help your entity identify, measure and monitor key risk areas in your contract portfolio through **a process of discovery and assessment**. This helps your organization focus in on present-day compliance but can also help you anticipate potential issues in the future.

Enable Strategies to Support your Mission—Develop a contract compliance strategy that aligns first, second and third lines of defense to understand potential risks and create solutions that support your mission, vision and values.

Educate Key Stakeholders—Educate your stakeholders on risk trends that affect your organization to improve decision making and increase the effectiveness of your resource allocations.

Gain 360° View of Your Contract Portfolio—Develop an understanding of your third-parties, the types of goods and services they provide to you, agreement terms and conditions, key performance indicators and/or reporting requirements, enabling your organization to have constructive conversations with, and reporting to, key stakeholders.

Risk Transformation—Develop a risk-based contract compliance monitoring plan that helps you better anticipate and identify potential issues, prioritize certain third parties, and ultimately reduce the burden of compliance activities, while increasing revenue / decreasing costs.

Organizations are going to be at varying levels of sophistication when it comes to contract oversight, based on the available people and technologies, as well as the contract portfolio.

Common contract oversight challenges

Lack of a central repository to maintain contracts and related documents	Complex and/or voluminous number of contracts	Evolving standards – regulatory landscape is constantly changing	Inability to share information among multiple stakeholders using the contract / operating in silos	Unclear contract terms and conditions
Complex and/or ambiguous rate tables	Inability to map between contract terms and vendor services/invoices	Inconsistent interpretation of contract terms between entity and vendor	High volume transactions and/or complex, long-term projects	Lack of training in contract set-up, execution, and oversight/administration
Poor quality of data/information provided from vendors, limiting transparency	Lack of internal data / integration among tools and technologies	Inconsistent and/or ineffective change management processes	It's time consuming, and there are limited resources available	

Assessing contract risk: example risk factors

Risk based approach

Each contract is structured differently and based on the type of contract and third party, different red flags (i.e., risk factors) exist and varying levels of monitoring may be needed.

Which contracts have the potential to disrupt your business if something goes wrong? A risk-based scorecard can be used to determine who to monitor more closely and/or who to audit and when and can be customized for each agreement type.

Third Party Scores

Risk Factors	Score	
Agreement complexity	2.2	0
Significance of agreement to the organization	3.3	0
Number of third-parties involved	1.0	0
Changes in key third-party personnel	1.5	0
Changes in third-party accounting systems	4.7	0
Performance compared to industry/market conditions	3.0	0
Changes in agreement terms	3.2	0
Timeliness of compliance by third-party	2.7	0
Lack of compliance by third-party	2.0	0
Mergers and acquisitions related to the third-party	1.0	0
New products or activities related to the third-party agreement	3.0	0

Summary of contract compliance oversight

- Document policies and procedures for contract oversight, including internal communication plans and contract document repositories.
- Assign ownership roles and responsibilities to contract owners. Provide relevant, comprehensive training to contract owners.
- Define who your vendors are/what contracts you have.
- Assess the risk the entity faces from contracts - either informally or formally through risk assessments.
- Perform, document, and report on oversight activities.
- Conduct internal and/or third-party audits.
- Follow-up on non-compliance to resolve past issues and ensure future compliance.

Internal and third-party contract compliance audits

Why organizations conduct contract compliance audits (both internal and third-party)

Reactive

- Many organizations believe that the due diligence prior to contracts being signed is sufficient to mitigate risk; typically, no further assessments are done until problems appear with the third parties
- Payments received are getting smaller or expenses/prices are increasing
- Third party is unresponsive to questions/lacks transparency
- Organization has information that the third party is non-compliant in some way (i.e. incorrect pricing, nonperformance)

Proactive

- Fiduciary responsibility to organization stakeholders
- Organization has developed a plan to monitor contract compliance
- Organization is looking to restructure the terms of the agreement
- Agreement will be expiring soon
- Induce future compliance

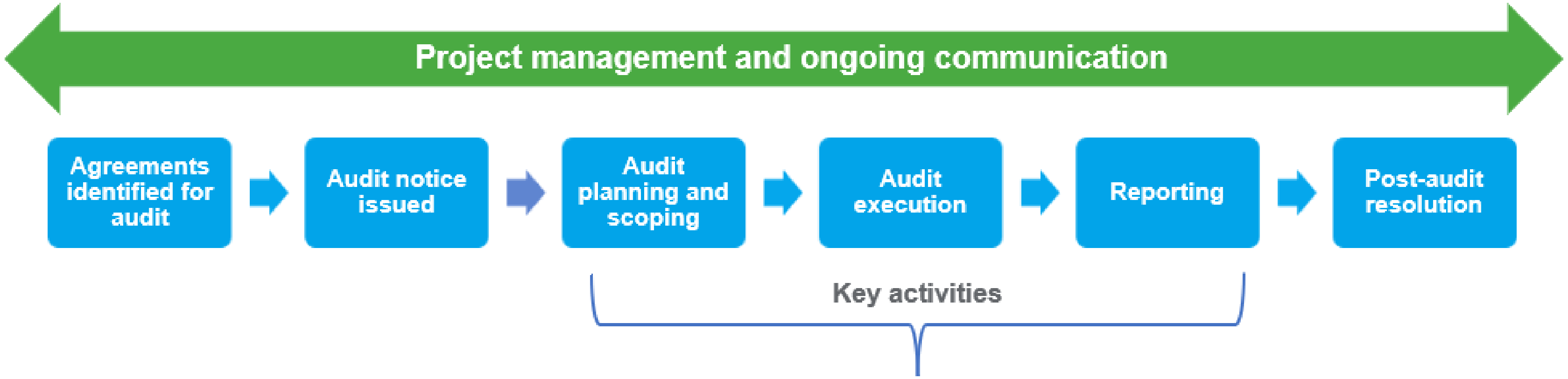
Most organizations are typically *REACTIVE* in nature, not *PROACTIVE*

Internal audits: example process and deliverables

Internal audit objectives typically focus on the organization's internal controls and performance related to contract monitoring oversight policies and procedures (and performance against those) related to the specific contract/vendor.

Third-party audits: example process and approach

Third party audit objectives typically focus on the third-party's compliance with terms and conditions of the contracts, including quantification of any monetary deficiencies/errors.



- Develop a project plan (scope, schedule, budget, etc.) with you to align expectations with all parties – as part of this we will define the key audit procedures to perform and collaborate with you to ensure we are focusing on the critical areas
- Establish a communication plan to define the preferred method and frequency of communications throughout the audits
- Gain a thorough understanding of the processes and existing relationship of each of the third parties examined
- Issue document request to the third party and complete planning activities based on initial information received
- Test compliance with the underlying agreement through review of supporting source documents and completion of analytical procedures
- Monitor performance relative to the project plan; routinely communicate status
- Analyze potential monetary exceptions and quantify impact
- Discuss initial findings and potential recommendations with you and the third-party
- Draft report and related findings and recommendations
- Deliver insights to management and collaborate on the development of practical corrective action plans, as appropriate

Common audit findings

1

NONCOMPLIANCE WITH CONTRACT TERMS

Noncompliance with agreed-upon terms and conditions, such as deliverables, timelines, pricing or quality standards, leading to breaches of contract.

2

LACK OF SUPPORTING DOCUMENTATION

Failure to maintain comprehensive records, including, but not limited to, contract documents, amendments, change orders, and invoices and corresponding supporting documentation, making it difficult to track obligations and verify compliance.

3

INVOICE REVIEW

Weaknesses in the design or implementation of controls for reviewing and validating invoices, leading to increased risk of errors, fraud, or non-compliance with contractual terms.

4

VENDOR MONITORING

Inadequate monitoring of vendor performance throughout the contract lifecycle, hindering the timely identification of issues and corrective actions.

5

PROCUREMENT

Violations of procurement policies and procedures, including lack of competitive bidding, favoritism, or conflicts of interest in vendor selection processes.

6

POLICIES AND PROCEDURES

Absence of documented policies and procedures, impeding the organization's ability to assess compliance and identify areas for improvement in contract management practices.

Case study: County elevator inspections internal audit

Background: Services contract to manage and perform the elevator inspections and review plans for new equipment installations for the County. For the 1-year review period, the County incurred third-party expenses for vendor inspection services in the amount of $722k and collected $1.7mil in inspection and permit fees.

Objective: Assess whether the system of internal controls is adequate and appropriate for effective contract compliance with selected provisions of the Contract as it relates to policies over elevator system review and approvals, inspections and permits, and identified contract terms.

Findings:

Non-compliant elevators in service

1,086 of the 2,937 (37%) elevator systems were non-compliant (due to failed inspection or unpaid fees) and therefore did not have valid elevator inspection certificates.

Policy non-compliance / vendor communication failure

There was $259k in unpaid inspection fees, even though County policy stated that fees had to be paid before inspection would occur.

Billing errors

The service descriptions and associated billing rates detailed in the contract rate chart did not consistently match the service descriptions and billing rates the vendor used on invoices.

Insufficient review of vendor invoices

Due to the limited functions of the County's software systems, there were no system generated reports of monthly inspections to utilize as to review completeness and accuracy of vendor invoices (which were over 40 pages per month).

Case study: School district parking services third-party audit

Background: Through a Resolution passed by the School District, the School District gave rights to operate parking services at certain locations to the vendor. In exchange, vendor was required to pay the District certain taxes on gross revenues related to parking services and submit payments on a monthly basis. The Resolution included audit rights of the parking vendor.

Objective: Determine the compliance of the vendor with contractual provisions related to the revenues and associated taxes paid to the District attributed to parking services.

Findings:

Unallowable deductions from revenue

The Resolution did not allow for any deductions from gross revenues to calculate the taxes due; however, the vendor did deduction certain amounts from gross revenues prior to calculating the taxes due to the District, resulting in $33,000 due to the District.

Late payments

34 of the 36 payments remitted to the District by the vendor during the Review Period were late, and subject to a six percent (6%) penalty fee in accordance with the Resolution. The District had charged the vendor for some late payment penalties during the period reviewed, but not all that were due, resulting in an additional $3,700 due to the District.

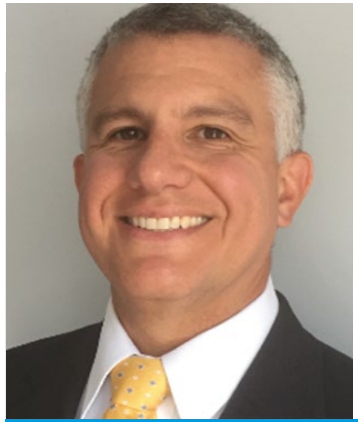
Questions

Thank you

Public Sector Continuity of Operations Planning (COOP)

RSM

Your instructors



Charles John

Director

Security & Privacy Risk Consulting, Chicago

Chuck has over 15 years of experience in the public sector leading teams dedicated to emergency management, public health, and continuity of operations at the federal, state, and local levels.

Alyssa Connick

Manager

Security & Privacy Risk Consulting, Boston

Alyssa has over 9 years of experience directing teams and building and deploying business continuity and disaster recovery programs in the public and private sectors.

Agenda

Min	Topic
5	Common terminology
40	Continuity of operations methodology
10	Case study
5	Questions

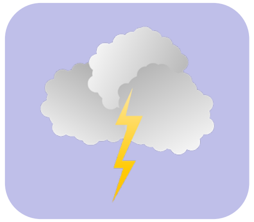
Objectives

By the end of this course, you will be able to:

- Distinguish the common terms of operational resiliency.
- Discuss the phases of continuity of operations in the public sector.
- Identify the primary planning components of public sector continuity and disaster recovery planning.

Common terminology

Common terminology



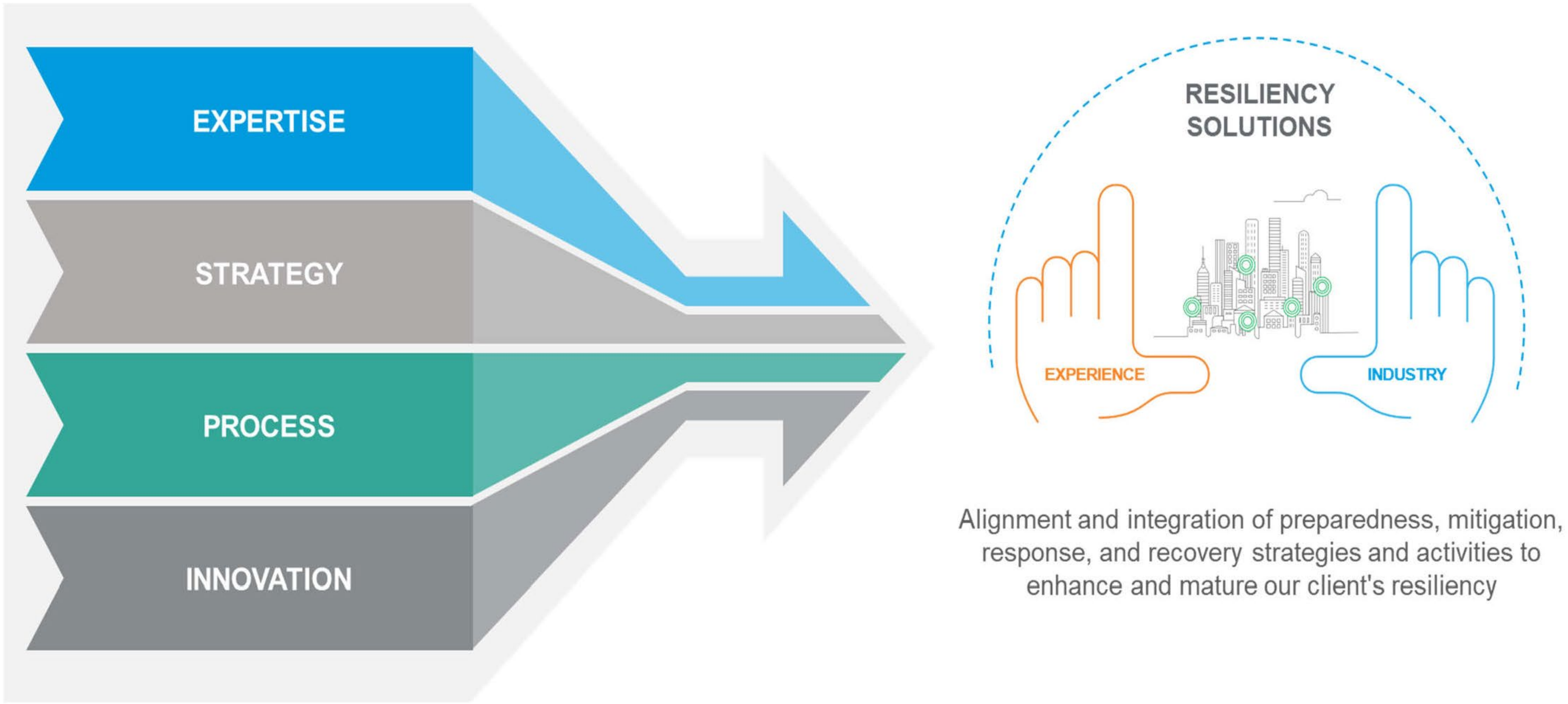
Emergency Response- **Emergency Response** (aka Crisis Management) is an immediate, systematic response to an unexpected or dangerous occurrence.

Continuity of Operations- Business Continuity identifies **mission essential work functions** and **critical supporting activities and resources** (e.g., systems and applications, staff, equipment, etc.) and develops strategies to maintain these essential work activities in the absence of critical supporting resources.

Disaster Recovery- Disaster Recovery identifies the **information technology** environment (infrastructure, hardware, systems, applications) and develops plans to facilitate recovery and restoration of the IT infrastructure.

Cyber Incident Response- Cyber Incident Response is an organization's strategies, activities, protocols, procedures, and technologies for detecting and responding to cyberthreats, security breaches or cyberattacks. *Identify, Protect, Detect, Respond, Recover*

Operational resilience



Continuity of Operations methodology

Building & enhancing COOP and DR programs in the Public Sector

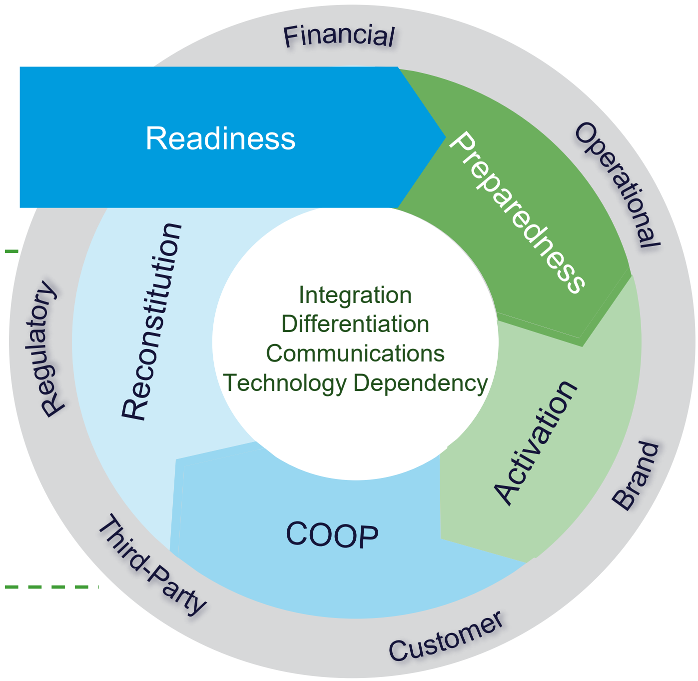
Continuity of Operations and Disaster Recovery methodology

Readiness

- Oversight and Support
- Alignment to EOP
- COOP and DR Roles and Responsibilities
- Plan Maintenance
- Governance

Reconstitution

- Alternate Location Devolution
  - Communication
  - Staff transition
  - Site breakdown
- Resumption to Daily Operations
- After Action Reporting



Continuity of Operations Plan

- Incident Command Expanded
- Shift to PMEF and MEF maintenance
- Activation of Alternate Locations
- COOP Staffing
- Disaster Recovery Plan
- Systems and Applications Runbooks

Preparedness

- Incident Command Structure
- Business Impact Analysis
  - Primary Mission Essential Functions (PMEF)
  - Mission Essential Functions (MEF)
  - Recovery Time Objectives (RTOs)
  - Recovery Point Objectives (RPOs)
  - Dependencies (Internal & External)
- THIRA
- Technical Impact Analysis
  - System and Applications Supporting PMEFs and MEFs
  - Recovery Sequence
- IT Disaster Recovery Strategies
- Alternate Work Locations
- Resource and Third-Party Strategies

Activation

- Continuity Plans and Procedures
  - Suspension of functions
- Alternate Locations and Relocation Plans
- Staffing Matrix
- Dependency Planning (e.g., Resource and Third-Party Strategies
- Disaster Recovery Strategies

Phased approach from readiness to reconstitution based on a combination of industry standards, field work, and industry experience

- **Readiness**
- **Preparedness**
- **Activation**
- **Continuity of Operations**
- **Reconstitution**

The RSM methodology, with supporting components, depicts the foundation of a comprehensive continuity of operations plan and disaster recovery plan.

BC and DR program maturity approximation

Not Developed

Level 0

- Control elements not yet developed, or there is no evidence that they exist.
- Impact of disruptive events is potentially catastrophic.

Basic

Level 1

- Control elements are initiating, or in their infancy.
- Approach to BC/DR planning is limited or ad hoc, with unclear ownership and/or oversight.
- Undefined roles and responsibilities.
- Impact disruptive events is potentially critical.

Evolving

Level 2

- Control elements are intuitive.
- The BC/DR program is evolving, expanding, and improving.
- Inconsistent processes and documentation.
- Some oversight, and incomplete roles and responsibilities.
- Limited communication between teams.
- Impact of disruptive events is potentially severe.

Established

Level 3

- Control elements are defined.
- BC/DR program is documented, with adequate support and clear ownership.
- Oversight, reviews, updates and tests are inconsistent.
- Critical business processes are known and RTOs and RPOs are documented.
- Roles and responsibilities are defined.
- Impact of disruptive events is potentially moderate.

Advanced

Level 4

- Control elements are in place and documented.
- Senior management involvement active and consistent.
- Extensive, controlled communication processes for internal teams and external entities.
- Roles and responsibilities are known.
- Timely exercises, training/awareness and plan update processes.
- Impact of disruptive events is potentially controlled.

Leading

Level 5

- Effective control elements are established and measurable.
- Program audits and plan updates are scheduled.
- Exercises are robust, and include both IT and business process personnel, lessons learned and follow up activities.
- Senior management provides strategic direction and guidance for BC/DR.
- Roles and responsibilities are known, understood and include both primary and secondary resources.
- Impact of disruptive events is potentially low.

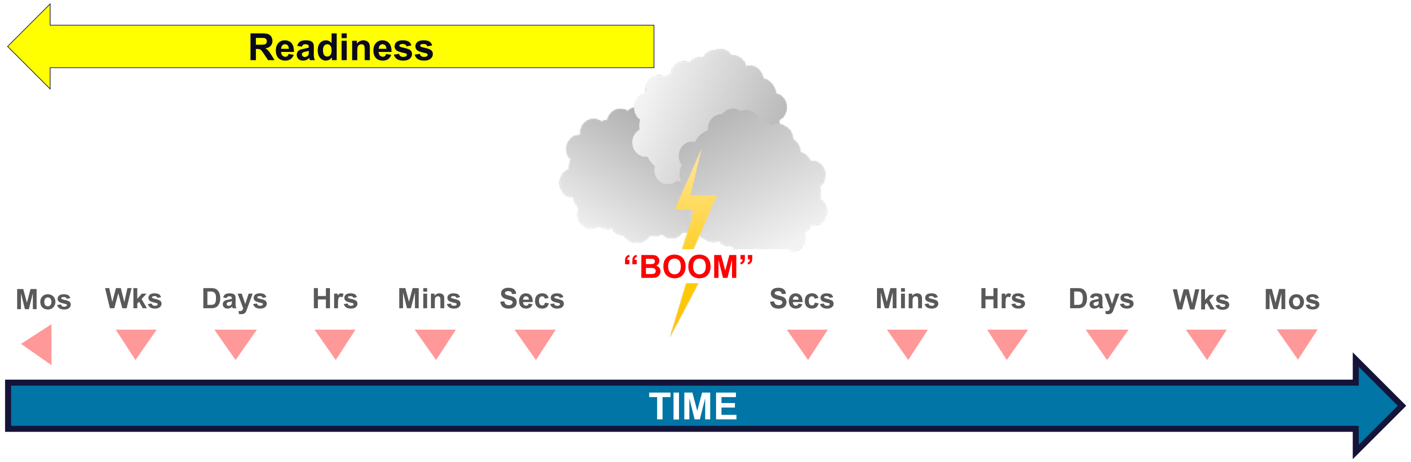
The approximate maturity categories for a business continuity and disaster recovery program, while subjective, are effective to estimating program status.

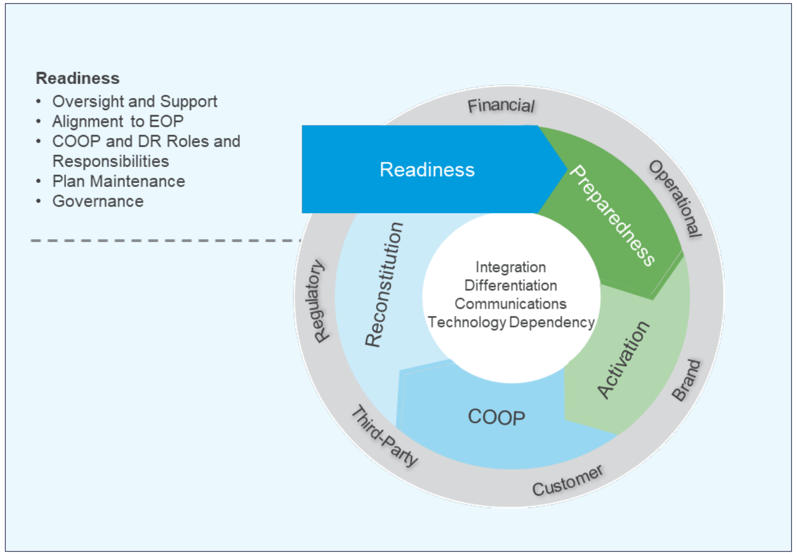
Readiness

Readiness

Popular phrase: “Left” and “right” of boom

- Readiness is “left” of boom
- These activities demonstrate the resiliency lifecycle ensuring a continuity and disaster recovery program receives and maintains leadership support and documentation is current and aligns to your EOP





For all practical purposes, your organization’s readiness never truly stops.

Readiness

- Oversight and Support
- Emergency Operations Plan Alignment
- Continuity and Disaster Recovery Roles and Responsibilities
- Plan Maintenance
- Governance

Oversight and support

- Leadership in the private sector usually must be "sold" on continuity planning with a budgetary line item.
- State and local government entities normally are mandated (in some way) to have a continuity of operations plan.
- State and local government leadership must act as "champions" to ensure continuity and disaster recovery planning is effectively maintained and operational.

The key to a successful Continuity of Operations Plan and a Disaster Recovery Plan is leadership's oversight and continued support.

Drivers – Getting leadership support

Readiness

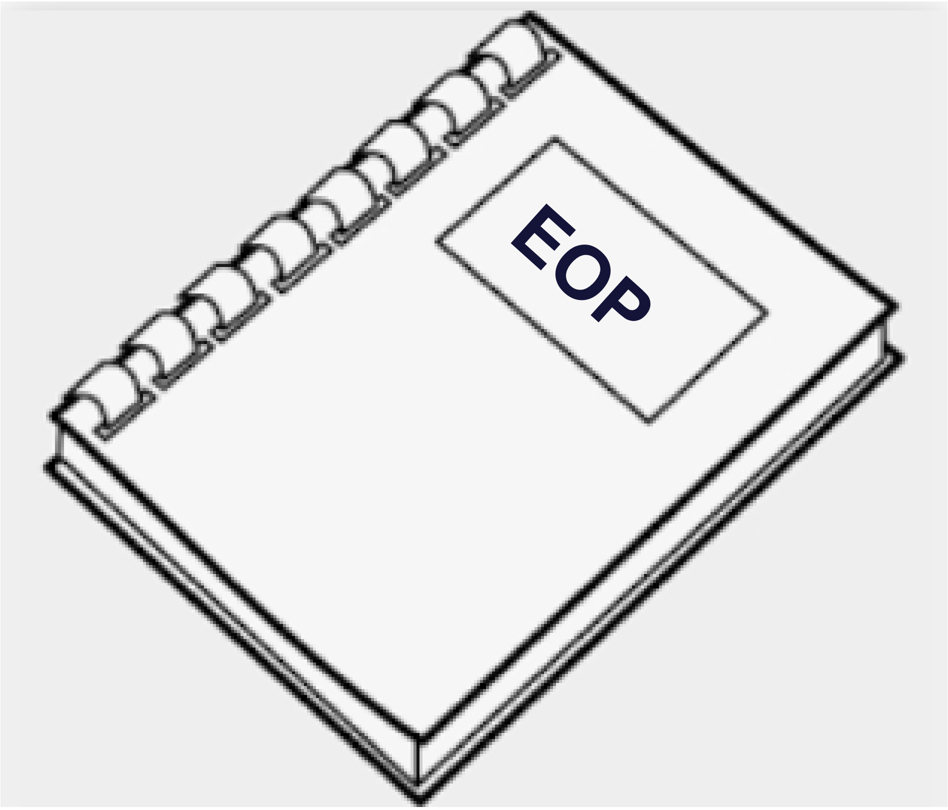
- Oversight and Support
- Emergency Operations Plan Alignment

- Continuity and Disaster Recovery Roles and Responsibilities
- Plan Maintenance
- Governance

Compliance	Grants administration, federal requirements, SOX reporting
THIRA/SPR	FEMA **T**hreat & **H**azard **I**dentification **R**isk **A**ssessment (states, territories, and tribes), FEMA **S**takeholder **P**reparedness **R**eview, mitigation plan
Real event or near misses	Natural disasters, system failures, infrastructure attacks, supply chain disruption
Vendors, suppliers	Third party risk management audit findings, supplier and vendor requirements, supply chain continuity

The frequency of cyber attacks and ransomware events alone should demonstrate the extreme need for an operational resiliency program (Crisis Management, Continuity of Operations, Disaster Recovery, and Incident Response).

Emergency Operations Plan alignment



- Historically, the continuity plan was treated as an appendix to the Emergency Operations Plan like the hazard appendices.
- As continuity planning evolved and disaster recovery emerged, COOP and Disaster Recovery are stand-alone plans.
- Suggested topics:
  - Scope and assumptions
  - Incident command structure
  - Individual teams with clear roles and responsibilities
  - Primary Mission Essential Functions to include staffing and critical resources and assets
  - Relocation activities
  - Resumption activities

The key to plan alignment is to ensure your incident command structure clearly depicts continuity and disaster recovery.

Readiness

- Oversight and Support
- Emergency Operations Plan Alignment

- Continuity and Disaster Recovery Roles and Responsibilities
- Plan Maintenance
- Governance

Roles and responsibilities examples

- **COOP Unit Leader (or Team Leader, Coordinator, etc.)**
  - Liaison to/from the Branch Director or Liaison to Operations Chief if COOP is its own Branch
  - Responsible for COOP activation
  - Coordination with the DR Team Leader
  - Provide COOP status for Operational Briefings
  - Responsible for maintaining COOP
  - Responsible for the COOP portion of the After-Action Report

- **COOP Unit (or Team) Members**
  - Execute PMEF, MEF critical activities
  - Provide situational awareness information to COOP Unit Leader (or Team Leader, Coordinator)

- **PMEF, MEF Leader**
  - Leads of the individual functions
  - Responsible for individual function COOP, notification of function staff following activation, and coordination of COOP activities

- **Disaster Recovery Team Leader**
  - Liaison to/from the Information Technology Branch Director
  - Responsible for DR Plan activation
  - Coordination with the COOP Unit Leader (or Team Leader, Coordinator, etc.)
  - Provide status of Disaster Recovery for Operational Briefings
  - Responsible for maintaining DR plan
  - Monitor disaster recovery activities through resolution, test and resumption
  - Responsible for DR portion of the After-Action Report

- **Individual Technical Teams**
  - Collaborate on plan(s) of action
  - Execute the recovery, test, and resumption strategies and activities (event dependent)

When developing the plans, ensure operational (i.e., action words) language is used for the roles and responsibilities.

Governance

Plan maintenance

- Annual review and approval by COOP Unit/Branch Coordinator and DR Team Lead
- Updates following real events, organizational changes

Leadership oversight

- Annual status update(s) to the General Command Staff
- Annual program update to COOP Unit/Branch Coordinator and DR Team Lead

Coordination

- Routine coordination of activities, exercises, after-action reports with Information Technology (or Continuity)

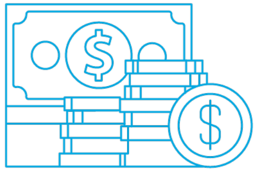
Plan governance is critically important to the success of the organization to respond, continue to operate, and recover from a disaster event.

Governance: Plan maintenance & industry tools

PUBLIC SECTOR

WebEOC
Riskonnect
Fusion

PRIVATE SECTOR



Riskonnect
ArcherIRM
Fusion
ServiceNow
Everbridge

- Tools promote governance and consistency across the organization in plan development and implementation.
- However, continuity and disaster recovery planning cannot be run or executed by a tool as experienced and trained staff are singularly the reason an organization can operate following a disaster event.
- All plans, especially continuity and disaster recovery, should not be governed by an industry tool as the tools cannot meet the unique needs of your organization.

If under-staffed, the tool can act as a self-service model enabling less staff to run and maintain the program (but awareness of the shortcomings is critical).

Readiness

- Oversight and Support
- Emergency Operations Plan Alignment

- Continuity and Disaster Recovery Roles and Responsibilities
- Plan Maintenance
- Governance

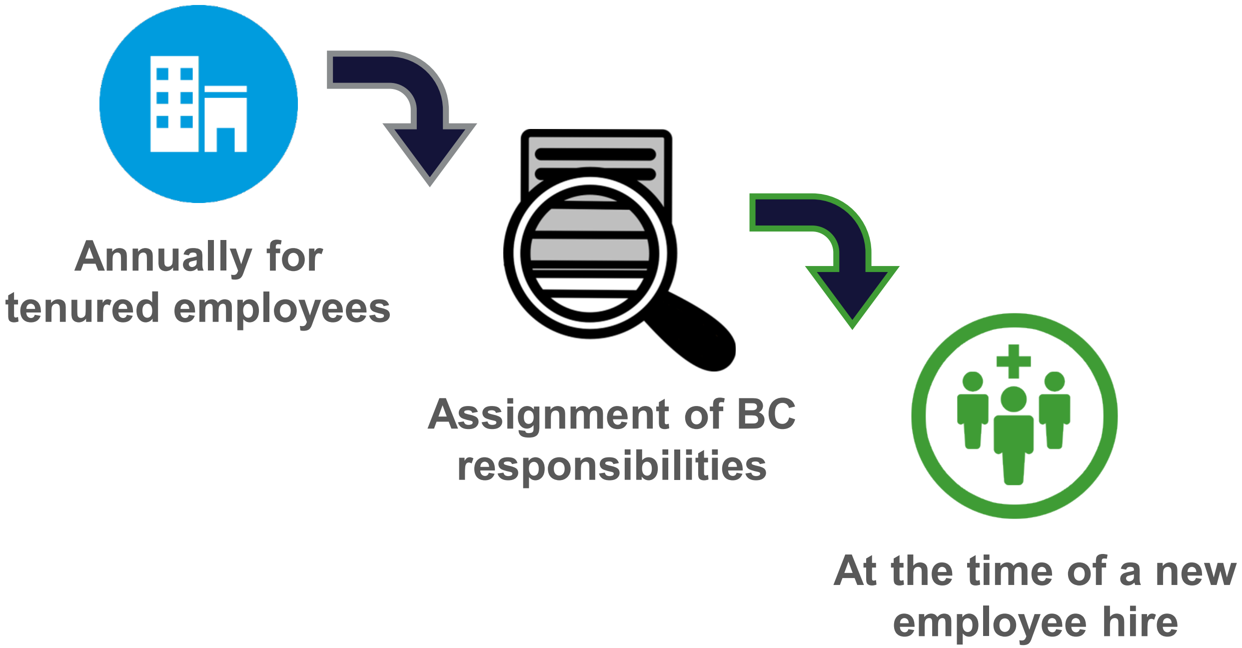
Governance: training and awareness

- One of the goals of COOP and DR training is to enhance resiliency throughout the organization by making resiliency part of the culture

- Training and awareness activities should be outlined in the Integrated Preparedness Plan (IPP; formerly MYTEP)

- Activities may include:
    - Live in-person or virtual training
    - Educational emails or documents
    - Themed weeks or months such as September (National Preparedness Month)

Training frequency



A comprehensive training and awareness program should align to the objectives of the planned exercises and be updated following exercises and real-events.

Governance: exercises and tests

Exercise planning
- Establish a planning team
- Document exercise objectives
- Document exercise scenario and scope
- Document exercise participants

Exercise execution
- Complete exercise
- Document strengths, weaknesses, opportunities and threats throughout the exercise

Reporting and remediation
- Develop an After-Action Report (AAR) with observations and recommendations
- Develop a remediation plan

- Homeland Security Exercise and Evaluation Program (HSEEP)
- Exercises should occur at least annually as laid out in the IPP
- The goal of exercises is to identify gaps in planning in a simulated environment
- Exercises can involve the entire organization or targeted to specific PMEFs or MEFs
- Exercises should not be pass/fail, and should document opportunities for improvement
- Best practice is to coordinate continuity and disaster recovery exercises

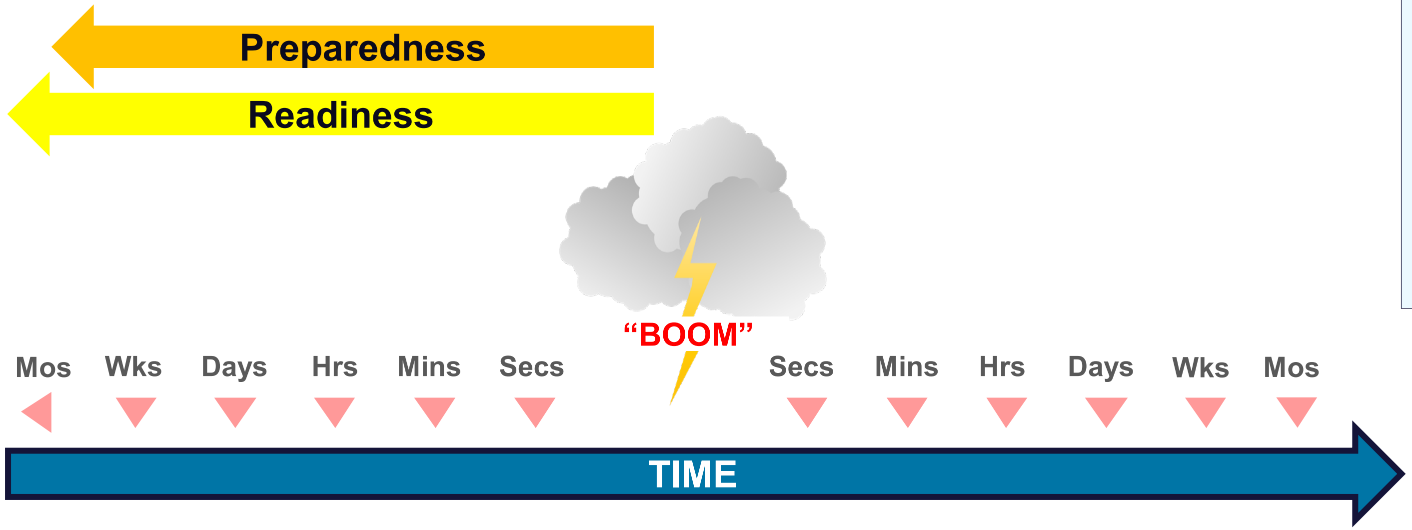
DHS FEMA provides a robust library of templates to conduct, design, develop, execute, and evaluate exercises as well as comprehensive improvement planning resources.

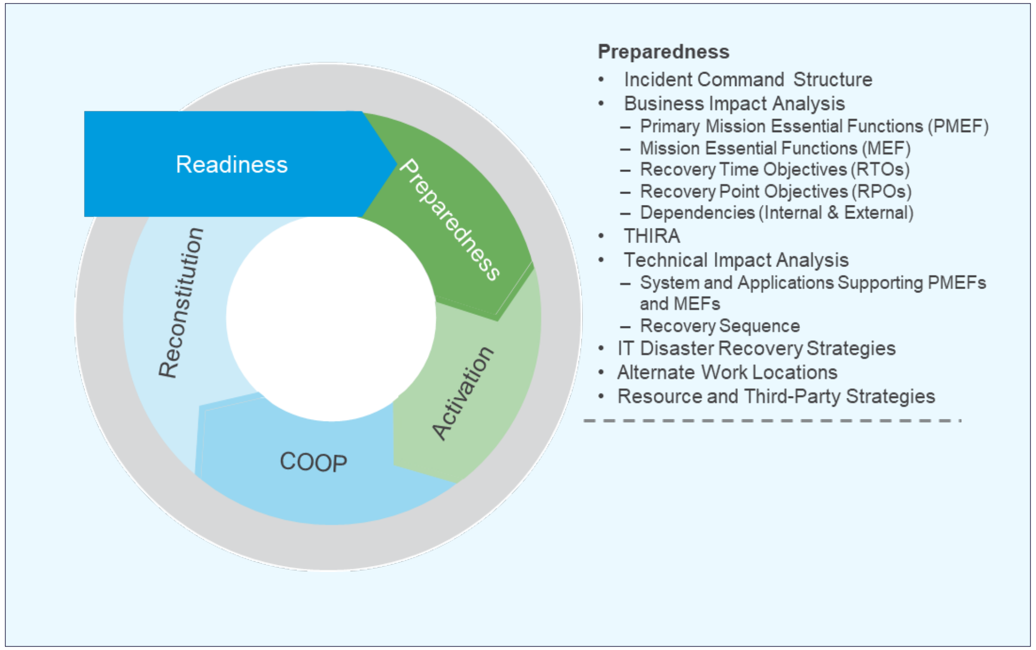
Preparedness

Preparedness: The event timeline

Popular phrase: “Left” and “right” of boom

- Preparedness is “left” of boom
- Largely, Preparedness activities are vitally important to maintain (i.e., keep up to date) once they are completed





Note: For the purposes of today’s discussion, Preparedness is depicted to stop at “boom” because it is described as a phase in the continuity and disaster recovery lifecycle.

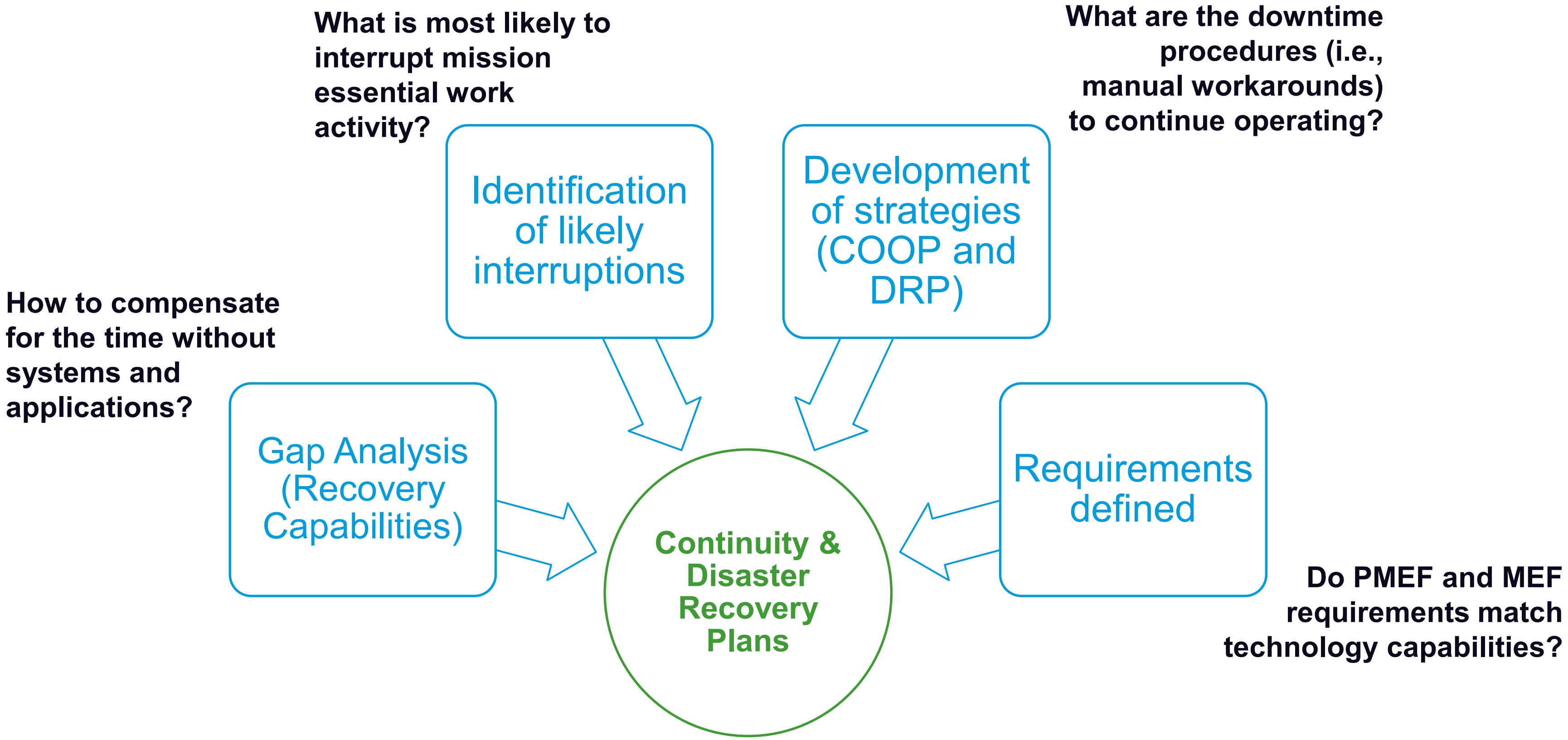
Preparedness never truly stops. Lessons learned from real-events and exercises heavily influence preparedness data and content contributing to the enhancement of your resiliency.

Preparedness process

Preparedness

- Incident Command Structure
- Business Impact Analysis
- THIRA

- Technical Impact Analysis
- IT Disaster Recovery Strategies
- Alternate Work Locations
- Resource and 3rd Party Strategies



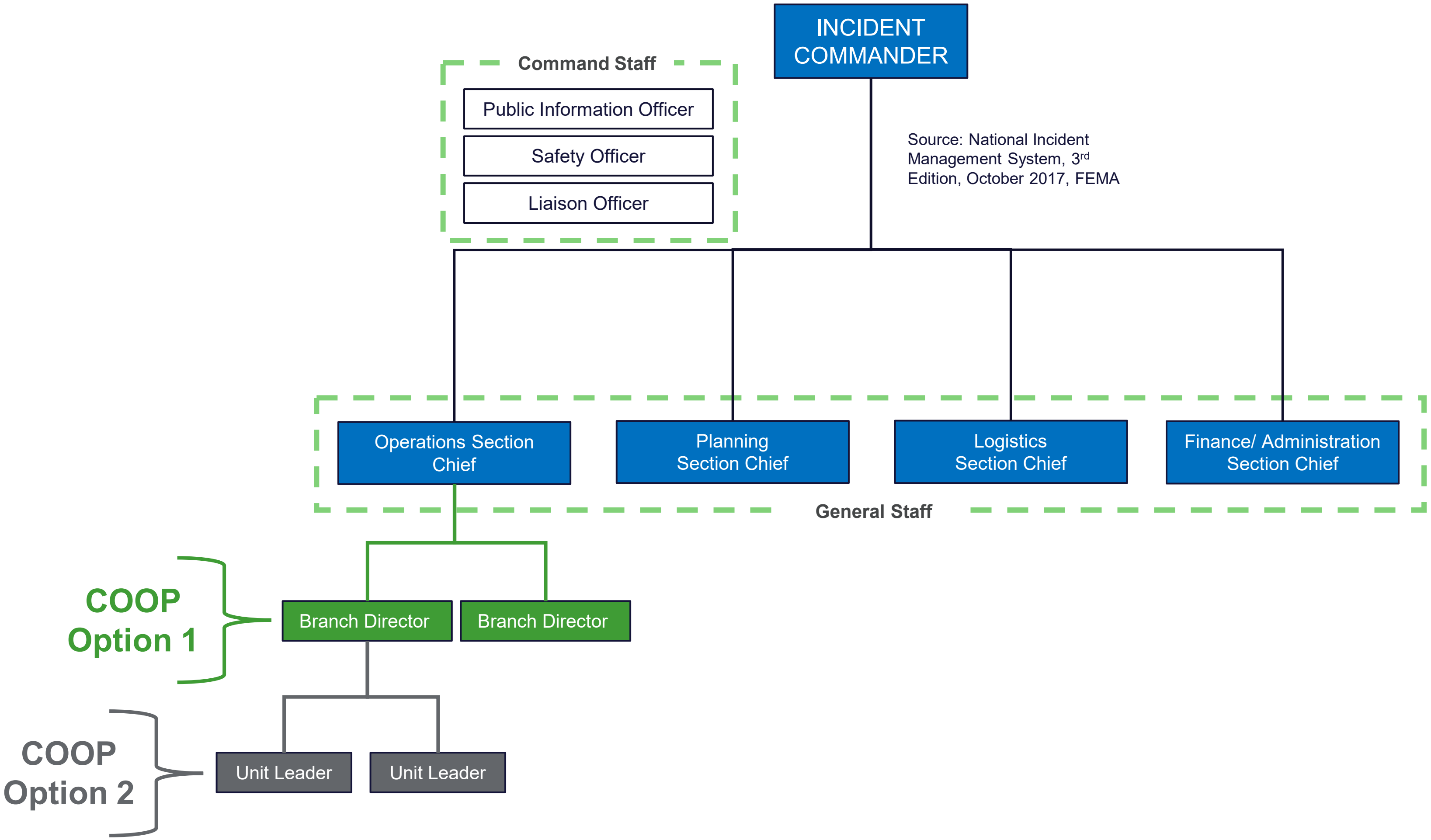
Business and technology requirements should be identified before developing any continuity and disaster recovery strategies and activities.

Incident command structure: Continuity of Operations

Preparedness

- Incident Command Structure
- Business Impact Analysis
- THIRA

- Technical Impact Analysis
- IT Disaster Recovery Strategies
- Alternate Work Locations
- Resource and 3rd Party Strategies

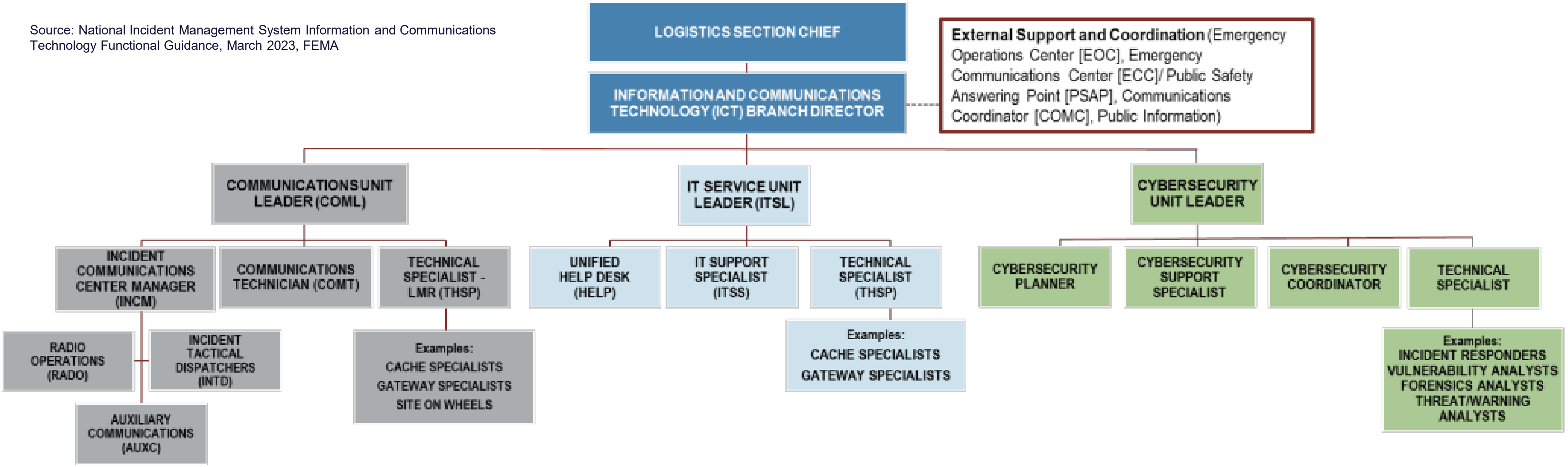


- Continuity of Operations Function (COOP)
- The scale of the disaster event generally determines if Continuity will be at a Branch Director or a Unit Leader level (**Option 1** or **Option 2**).

Continuity of Operations falls under the Operations Chief. COOP may be a Branch or a Unit - the precise positioning is based on the organization and the type and breadth of the disaster event.

Incident command structure: Disaster recovery

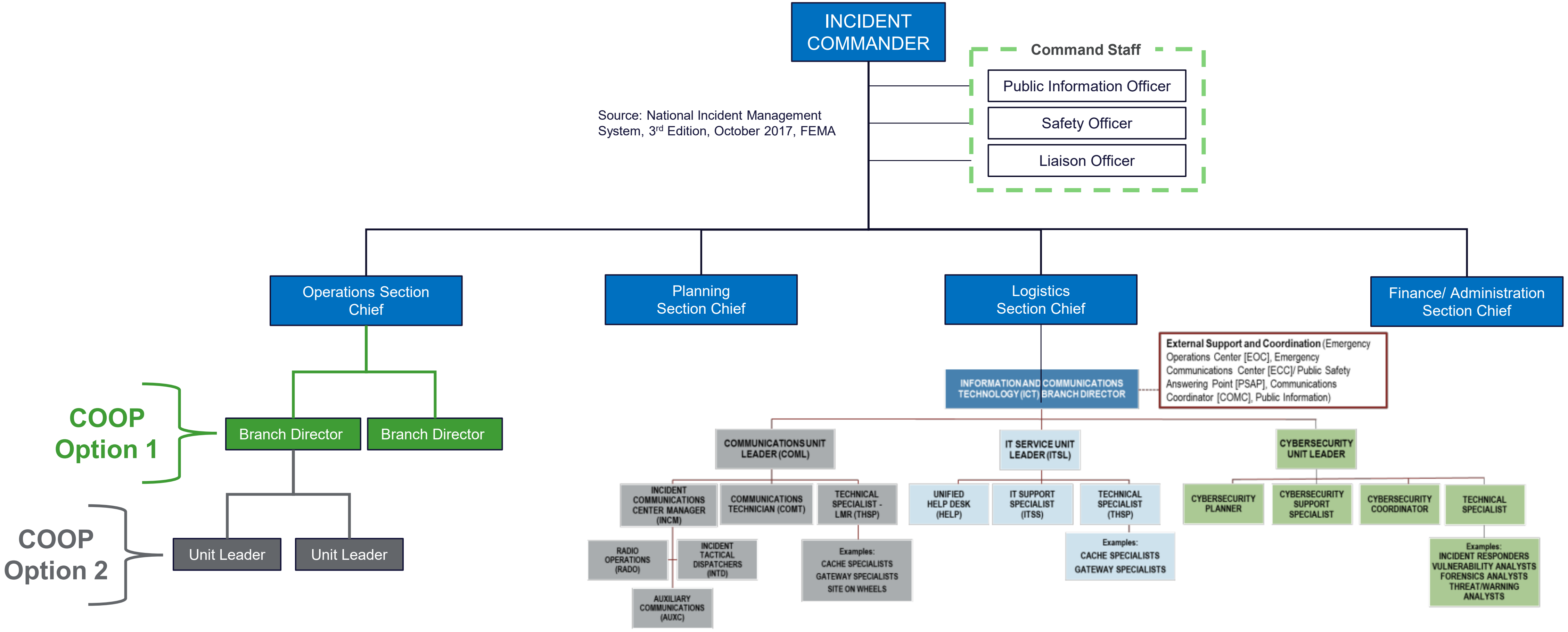
Source: National Incident Management System Information and Communications Technology Functional Guidance, March 2023, FEMA



- ICT Function (Information and Communications Technology)
- Communications, Information Technology Service and Cybersecurity may be organized under the ICT Branch Director under the Logistics Section Chief

Disaster Recovery is part of the Information and Communications Technology Branch. The ICT Branch is under the Logistics Section Chief.

Incident command structure: Big picture



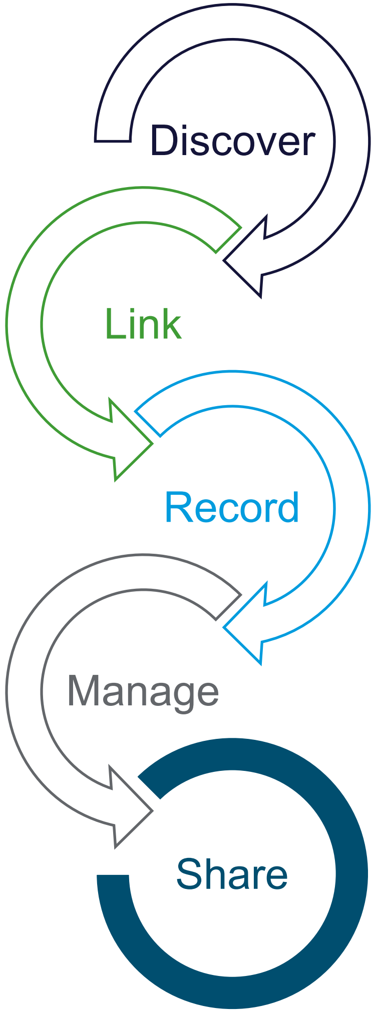
COOP Branch Director (or Unit Leader) and ICT Branch Director coordinate awareness and activities along with the Operations and Logistics Section Chiefs.

Preparedness

- Incident Command Structure
- Business Impact Analysis
- THIRA

- Technical Impact Analysis
- IT Disaster Recovery Strategies
- Alternate Work Locations
- Resource and 3rd Party Strategies

Business Impact Analysis (BIA)



Government: Identify the Primary Mission Essential Functions (PMEFs) and the Mission Essential Functions (MEFs)

Business (Revenue Generators): Identify the Critical Business Functions and the Suspended Business Functions

Map the Critical Activities to each Primary Mission Essential and Mission Essential Function or Critical Business Function.

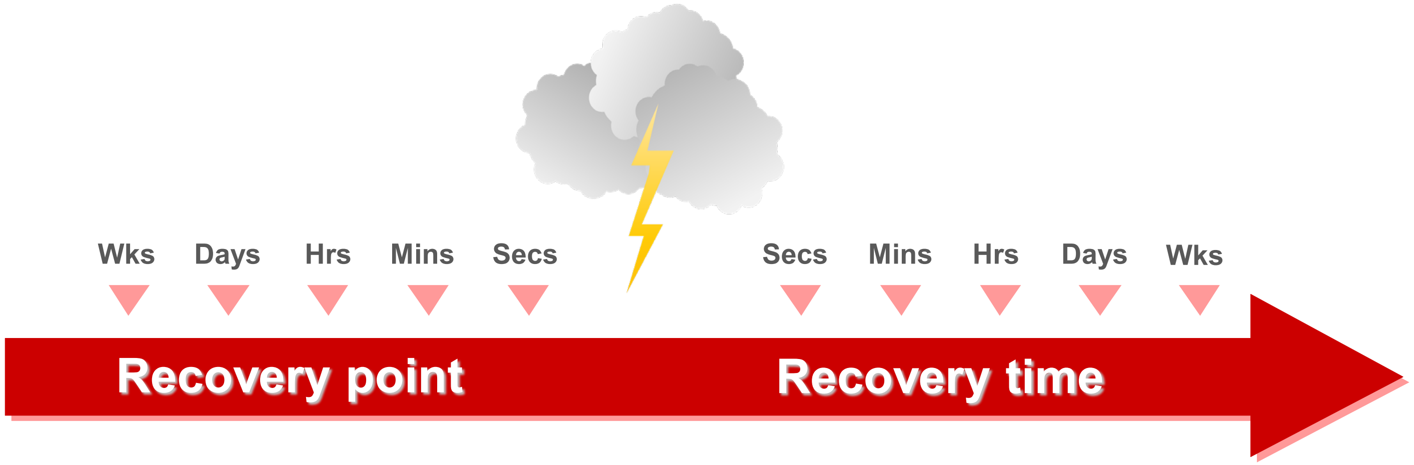
Document the critical resource requirements, such as the systems and applications, mission critical assets, mission critical staffing, internal and external dependencies, 3rd party vendors, suppliers, contractors

Establish recovery priorities (recovery time objective, recovery point objective, and other thresholds)

Collaborate with Information Technology by sharing recovery priorities and document gaps between expected and actual recovery capabilities

The business impact analysis should be reviewed and approved annually. Best practice is to perform a comprehensive BIA every 3 years.

Recovery metrics definitions



Recovery point objective (RPO) - Data

Point to which information used by an activity must be restored to enable the activity to operate on resumption. Can also be referred to as “maximum data loss” (ISO 22301). Identified as part of the BIA process.

Recovery time objective (RTO) - Availability

Time goal for the restoration and recovery of functions or resources based on the acceptable downtime and acceptable level of performance in case of a disruption of operations (ASIS). Identified as part of the BIA process.

Low RPOs and RTOs

- 0-1 hours
- 0-12 hours
- 24 hours

High RPOs and RTOs

- 72 hours
- 4-7 days
- 2 weeks or more

Systems and applications users must know the RTOs and RPOs to develop effective operational downtime (i.e., workarounds) procedures in the absence of technology.

Preparedness

- Incident Command Structure
- Business Impact Analysis
- THIRA

- Technical Impact Analysis
- IT Disaster Recovery Strategies
- Alternate Work Locations
- Resource and 3rd Party Strategies

Threat and hazard identification and risk assessment

1

Identify the threats and hazards of concern

Identification of threats across a jurisdiction, multi-jurisdiction, region for states, territories, and tribes

2

Give the threats and hazards context

Threats and hazards risk assessment for natural, technological, human-caused

3

Establish capability targets

Level of capability needed for preparedness, capability gaps, and mitigation of the gaps

4

Apply the results

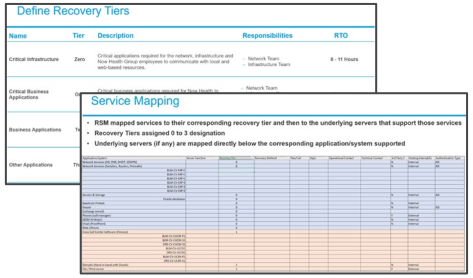
Address gaps by building and sustaining capabilities

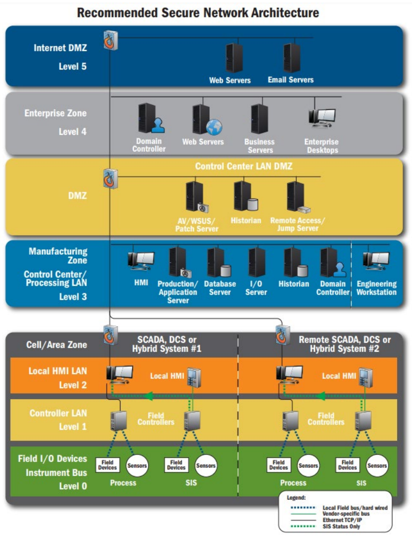
The 3 steps of the THIRA are to be repeated every 3 years.

Technology preparedness

IT Disaster Recovery strategies

- Identify the IT recovery capabilities based on the infrastructure, staffing, and service licensing agreements.
- Strategies form a consistent disaster recovery planning framework aligning response coordination, technology infrastructure documentation, and recovery activities.
- This framework identifies the critical Information Technology environment assets (network, systems, and applications) that support Primary Mission Essential Functions (PMEFs) and Mission Essential Functions (MEFs) to be recovery and restored following a significant interruption or outage.





IT recovery capabilities

- Inform the actual capabilities to recover on prem, SaaS, cloud, and 3rd party systems and applications as well as network components, which may differ from the user's expectations.
- Map systems and applications supporting PMEFs and MEFs.
- Identify the infrastructure needed to enable efficiency recovery.

Recall terminologies – disaster recovery pertains to the technology infrastructure and is NOT to be confused with cyber incident response.

Preparedness

- Incident Command Structure
- Business Impact Analysis
- THIRA

- Technical Impact Analysis
- IT Disaster Recovery Strategies
- Alternate Work Locations
- Resource and 3rd Party Strategies

Alternate work & resource strategies

Alternate locations

COOP

Maintaining operational capabilities

Maintaining PMEFs and MEFs at the alternate location with the right balance of inhouse and 3rd party resources (i.e., vendor continuity), role-based staffing reallocation, and operational checklists will ensure efficiency in standing up an alternate work location.

Reconstitution

De-mobilization

- Once the Incident Commander announces a return to daily operations, Reconstitution planning must include plans, procedures, protocols to break-down the alternate location and account for all staffing, resources, and assets.
- De-mobilization plans should be developed during the Alternate Work planning.

Alternate location planning

- Identify the alternate location ensuring the space is large enough to hold the incident command team as well as the support staff and compliance with environmental safety and security standards.
- Determine the business and information technology infrastructure and resources and assets needed to stand-up the alternate location.
- Formalize any additional (or emergency) procurement language necessary if additional resources and assets require purchasing.
- Document the staffing plan.
- Ensure any union contracts associated with any staff have been provisioned to include language permitting movement and work at an alternate location.

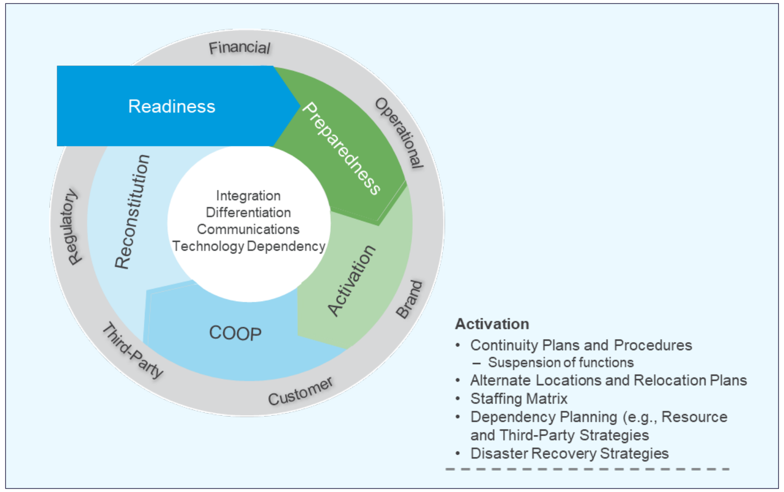
Third party vendor continuity planning is critical in your organization's ability to maintain PMEF and MEF.

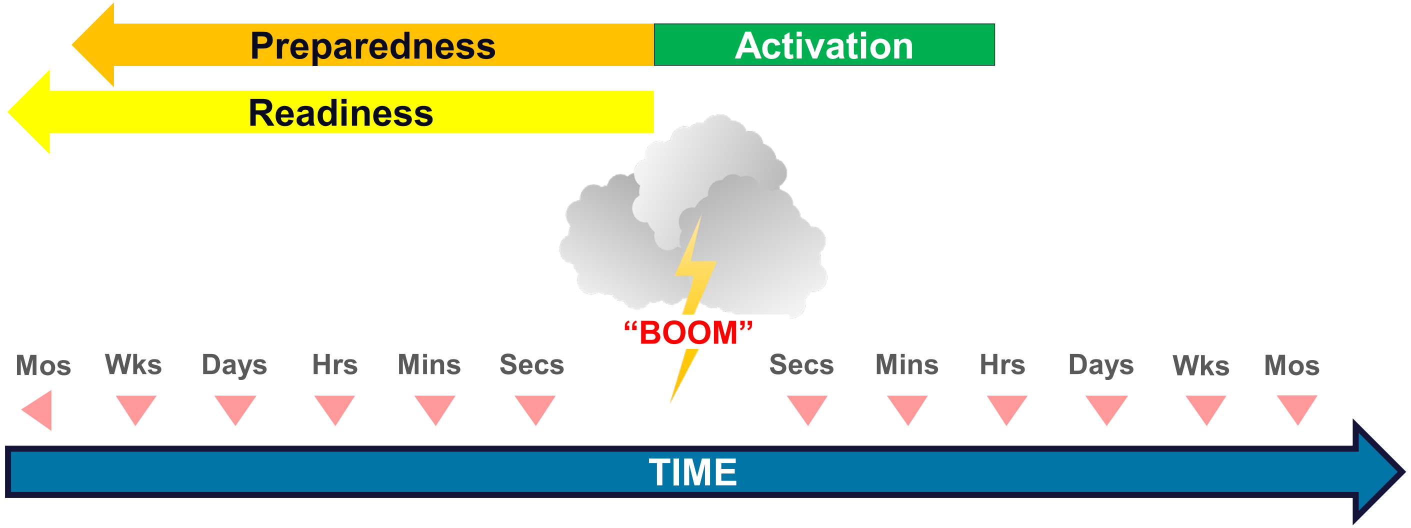
Activation

Activation: The event timeline

Popular phrase: "Left" and "right" of boom

- Activation is "right" of boom
- The COOP activation can occur at any point after EOP activation, initial situational assessment, and the immediate activation of the command group.





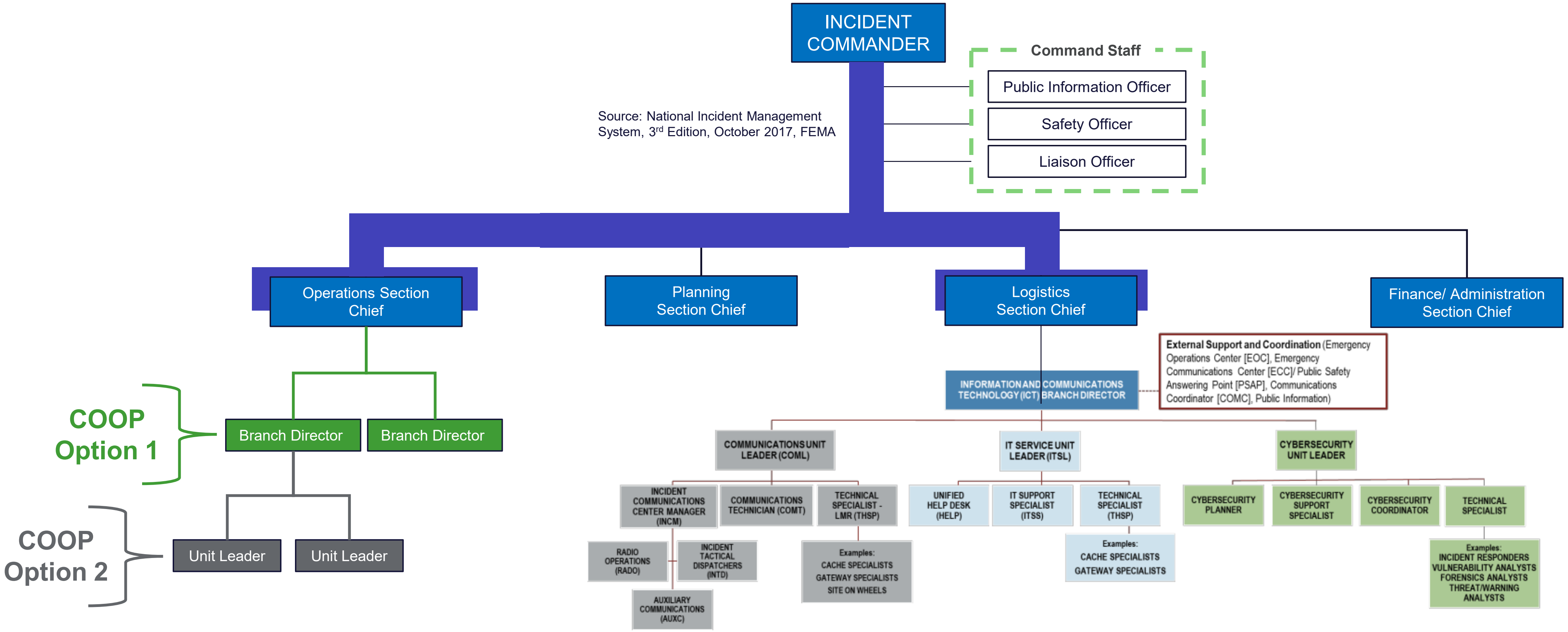
The COOP may be activated at any time following the disaster event. At a minimum, COOP activation depends on the type, breadth, and impact of the event.

Activation pathway

Activation

- Continuity Plans & Procedures
- Alternate Locations & Relocation Plans
- Staffing Matrix

- Dependency Planning – Resource & 3rd Party Strategies
- Disaster Recovery Strategies



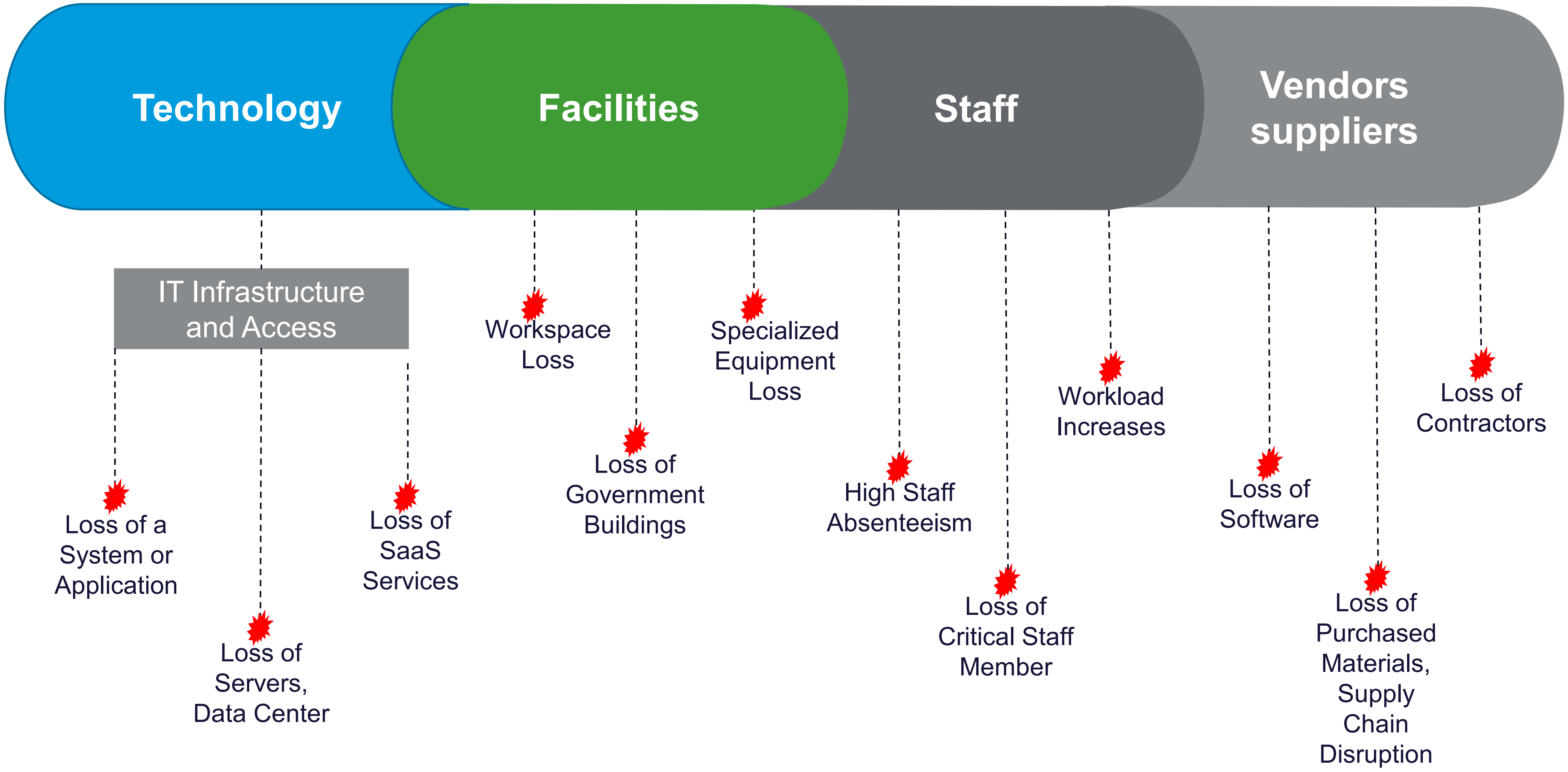
Based on the event, COOP and DR plans are activated by their respective branch directors in coordination with the Operations and Logistics Section Chiefs.

Activation

- Continuity Plans & Procedures
- Alternate Locations & Relocation Plans
- Staffing Matrix

- Dependency Planning – Resource & 3rd Party Strategies
- Disaster Recovery Strategies

Potential disruptions



These example disruptions across state, local, tribal governments and other public sector organizations can have devastating community impacts.

Activation

- Continuity Plans & Procedures
- Alternate Locations & Relocation Plans
- Staffing Matrix

- Dependency Planning – Resource & 3rd Party Strategies
- Disaster Recovery Strategies

Disruption strategy development

Technology
- Loss of a system or application
- Loss of major technology infrastructure (VPN, Data Center)
- Loss of SaaS services

Disaster Recovery Strategies
- Track information in excel and manually develop reports
- Work offline using files stored in alternate location
- Contact alternate vendor

Facilities
- Loss of workspace
- Government buildings
- Specialized equipment

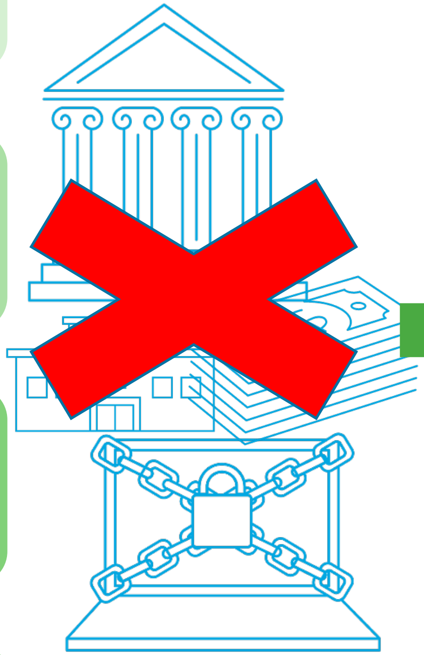
Alternate Location and Relocation
- Transition to work from home
- Engage Contracted manufacturing organization
- Transition operations to secondary facility

Staff
- High staff absenteeism
- Loss of critical staff member
- Increase in workload

Staffing Matrix
- Modified scheduling
- Leverage training documents
- Borrowed support from other areas of the business

Vendors, Suppliers, Contractors
- Loss of software
- Loss of purchased materials, supply chain disruption
- Loss of contracted staff

Dependency Planning
- Engage alternate vendor



CONTINUED OPERATIONS

Strategies to mitigate these example disruptions bolster your organization's resiliency and mitigate impacts of significant disaster events.

Strategy approval

Continuity and disaster recovery strategies MUST be approved by:

- Senior management and/or leadership
- Staff identified at the ICS Chief, Branch, and/or Unit leader positions

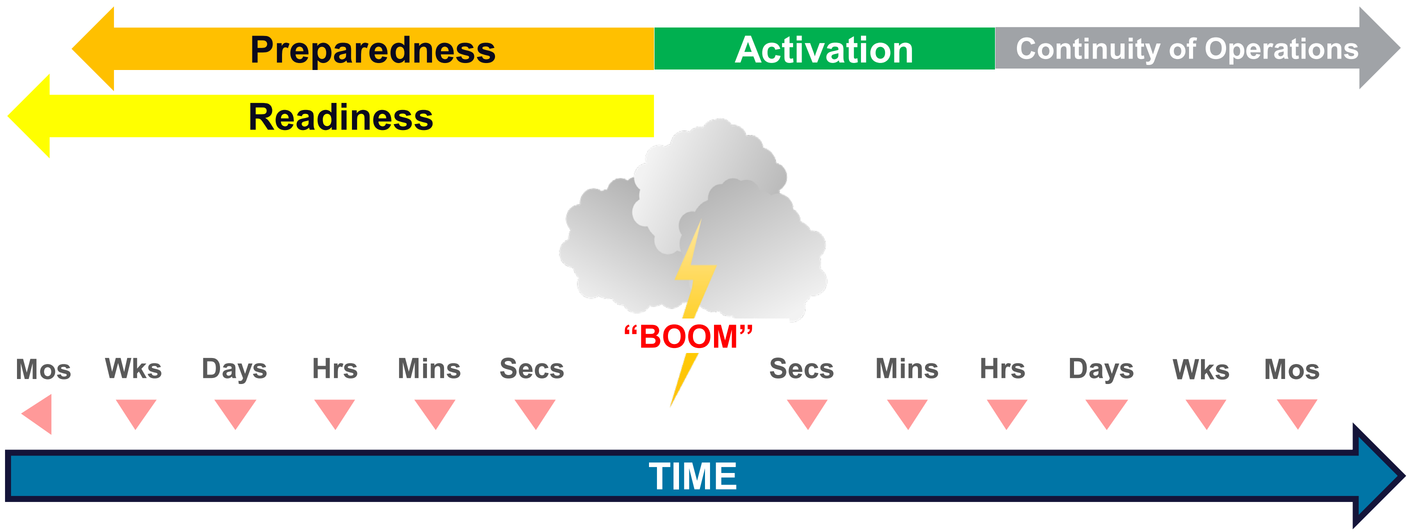
Senior level approvals ensure continuity and disaster recovery strategies align to support primary and mission essential functions.

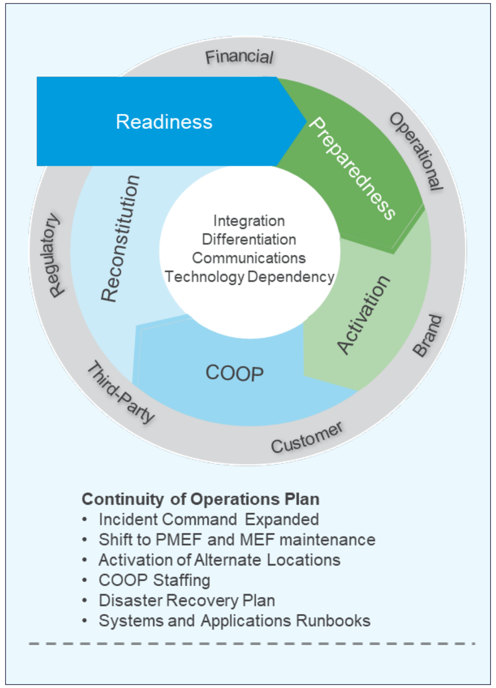
Continuity of Operations Plan

COOP: The event timeline

Popular phrase: "Left" and "right" of boom

- Continuity of Operations is "right" of boom
- Refers to the phase of Continuity of Operations as opposed to the continuity plan





The COOP may be activated at any time following the disaster event. At a minimum, COOP activation depends on the type, breadth, and impact of the event.

COOP

- Incident Command Expanded
- Shift to PMEF and MEF Maintenance
- Activation of Alternate Locations

- COOP Staffing
- Disaster Recovery Plan Activation
- Systems and Applications Runbooks

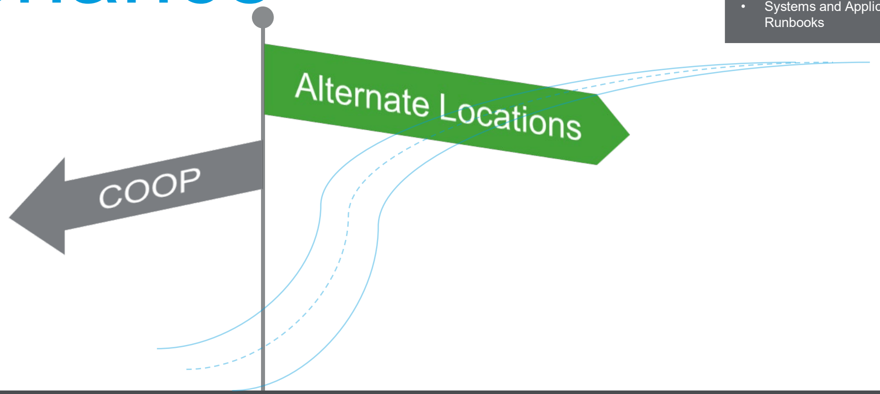
Shift to PMEF and MEF maintenance

The Business Impact Analysis (BIA) activities identified during Preparedness

Transition to PMEF and MEF (with the devolution of non-mission essential functions).

- (If needed), activation of relocation facility(ies) plans
- Staffing
- Resources/assets including telecom and IT functionality
- Vendors and their contact information

Follow plans on the devolution – all non-mission essential functions cannot be suspended at the same time. Sequence to devolve is needed along with the staff being moved.



Business Impact Analysis (BIA)

Non-Revenue Generating	Revenue Generating
Primary Mission Essential Functions	Critical Business Functions
PMEF Support Activities	Critical Activities
Mission Essential Functions	Suspended Functions
MEF Support Activities	Staffing Reallocation
Continuity of Operations Plan	**Business Continuity Plan**

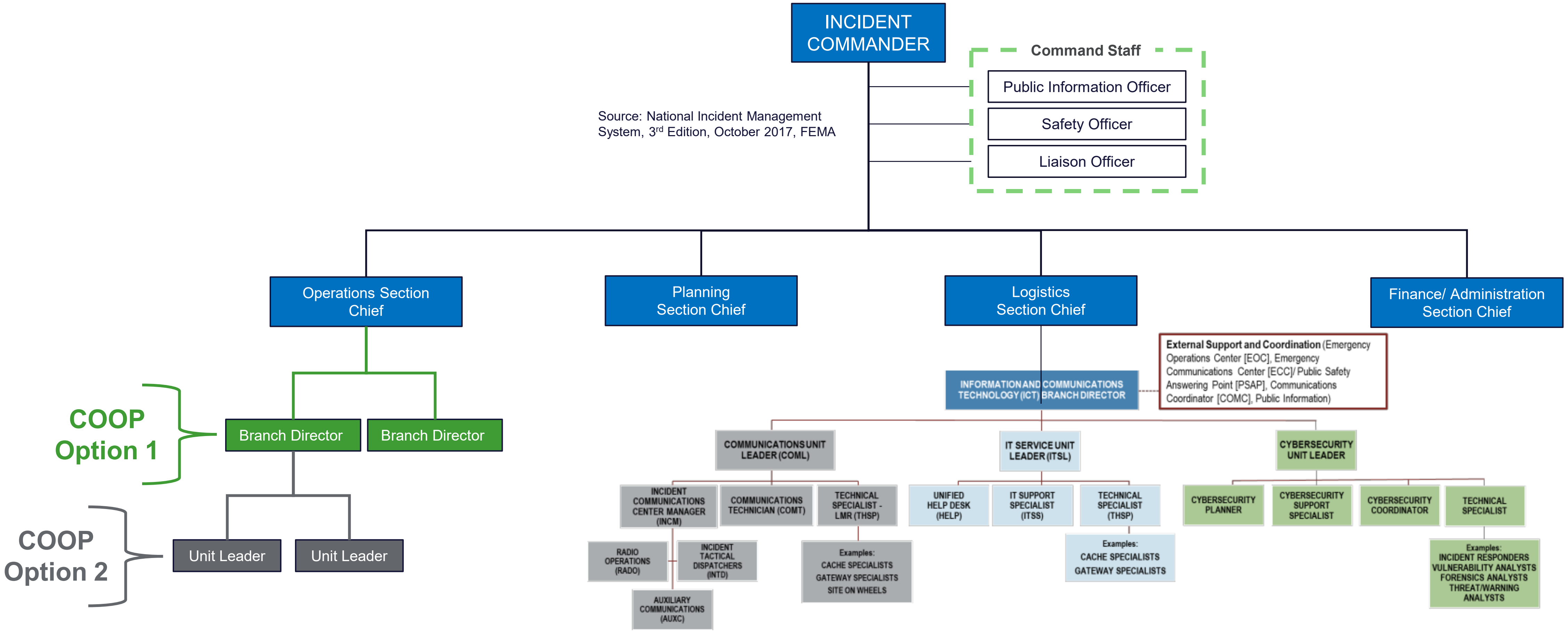
The immediate operational actions are transition to maintaining the mission essential functions, ensuring adequate staffing support, and the decision on standing up the alternate location.

COOP

- Incident Command Expanded
- Shift to PMEF and MEF Maintenance
- Activation of Alternate Locations

- COOP Staffing
- Disaster Recovery Plan Activation
- Systems and Applications Runbooks

Incident command expanded



COOP Branch Director (or Unit Leader) and ICT Branch Director coordinate awareness and activities along with the Operations and Logistics Section Chiefs.

Disaster Recovery Plan activation

Activation

- Assessment of reported event.
- Determination of whether to activate the Disaster Recovery Plan.
- Activate the ICT Branch Director.

Notification

- Notification pathway should be an expansion of the existing notification pathway in the Emergency Operations Plan.
- ICT Branch Director notifies IT Services Unit Leader.
- The Incident Command will expand as needed based on the event.

Respond

- Identify and analyze evidence to activate appropriate IT specialists based on impacts.
- Coordinate various work streams.
- Send internal notifications to staff.
- Determine involvement of external vendors.

Recover

- Criticality to recovery PMEF and MEF systems and applications.
- Leverage recovery documentation, such as:
  - System architecture
  - Recovery sequence guides
  - Systems and applications runbooks

Restore

- Once the impacted system(s) and/or application(s) has been recovered, verify and validate data and performance.
- Restore the IT environment to daily operations.
- Complete after-action report.

Continuity lead should be notified as part of the Disaster Recovery Plan activation for awareness and coordination to ensure PMEF and MEF are maintained.

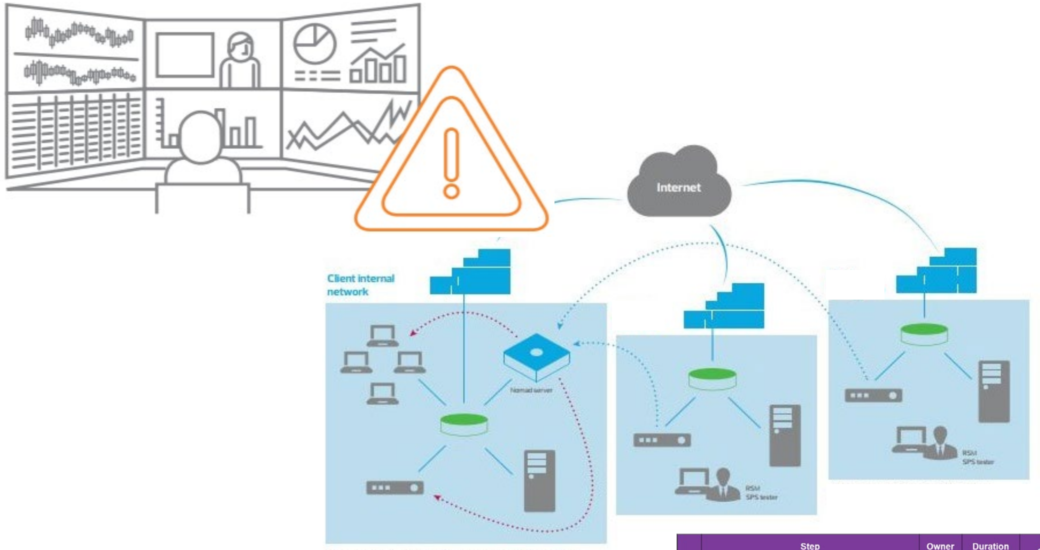
Systems and applications runbooks

- The Sequencing Guide should be used to organize critical recovery information for systems and applications and the order in which the systems and applications should be recovered.

- All critical information must be identified, and Information Technology must establish and confirm the recovery tiers.

- The systems and applications are identified as part of the BIA.

- If the BIA is not comprehensive, then the recovery sequence will not be accurate.



	Step	Owner	Duration	Recovery Components
1	Login to the Veeam application	TBD	TBD	Populate Veeam deployment IP address
2	Using the Backup Browser select the VM you are looking to recover	TBD	TBD	TBD
3	Select the restore point you are looking to recover.	TBD	TBD	TBD
4	Select the restore mode based on the current state of VMware hardware	TBD	TBD	TBD
5	Target the correct cluster (IT vs OT) to restore the target VM	[illegible]	[illegible]	[illegible]
6	Select the correct storage [illegible] VM	[illegible]	[illegible]	[illegible]
7	Restore the VM (A prefix or suffix) [illegible] the original VM is left on the hosts	TBD	TBD	TBD
8	Ensure the VM is attached to the correct network	TBD	TBD	TBD
9	Power on recovered VM and ensure the OS has network and auth connections	TBD	TBD	TBD
10	vSphere Cluster: Add new host to cluster root resource pools	TBD	TBD	TBD
11	vSphere Cluster: Leverage VMware VMotion to move select VMs to new host to load balance resources	TBD	TBD	TBD

	Step	Owner	Duration	Recovery Components
1	Operators to report disruption to I and E	Operators	Dependent on outage	Dependent on outage
2	I and E will troubleshoot or identify problem and request support from XX if necessary	I and E	Dependent on outage	Dependent on outage
4	For hardware failures, request a replacement part from City • For Warehouse pick up- I and E can retrieve part • For DCS Storage pick up • For hardware that needs to be shipped- City will overnight if necessary	I and E	Dependent on outage	Dependent on outage
5	For a failed computer, used the XX System Recovery guide to recover the computer	I and E	Dependent on outage	Dependent on outage

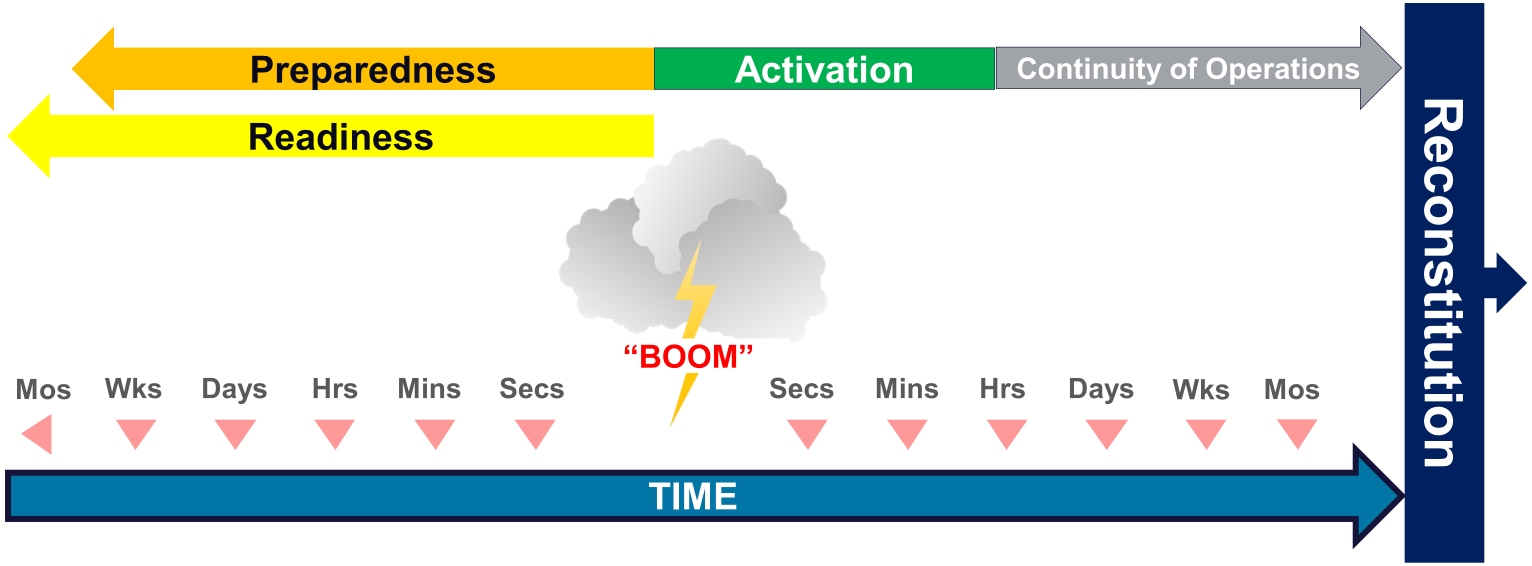
Coordination between the Continuity Branch and the ICT Branch is vital for operational downtime activities to account for IT outages to maintain PMEFs and MEFs.

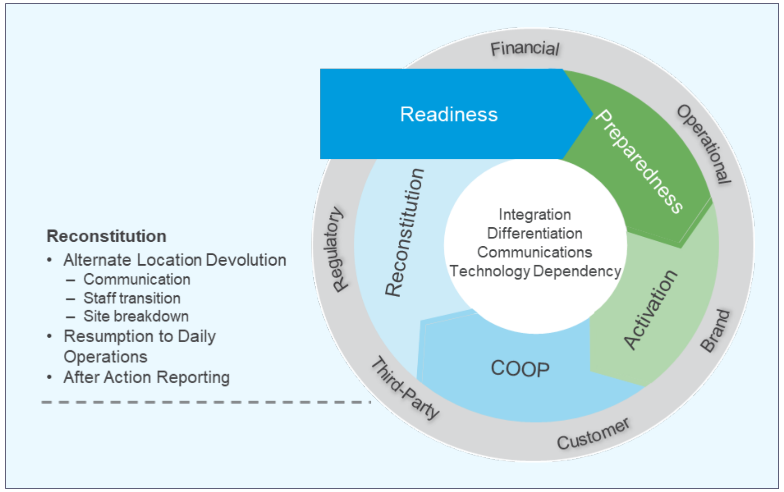
Reconstitution

Reconstitution: The event timeline

Popular phrase: "Left" and "right" of boom

- Reconstitution is "right" of boom
- Beginning with the Readiness Phase, reconstitution (i.e., resumption) of functions – return to daily operations – generally receives less attention





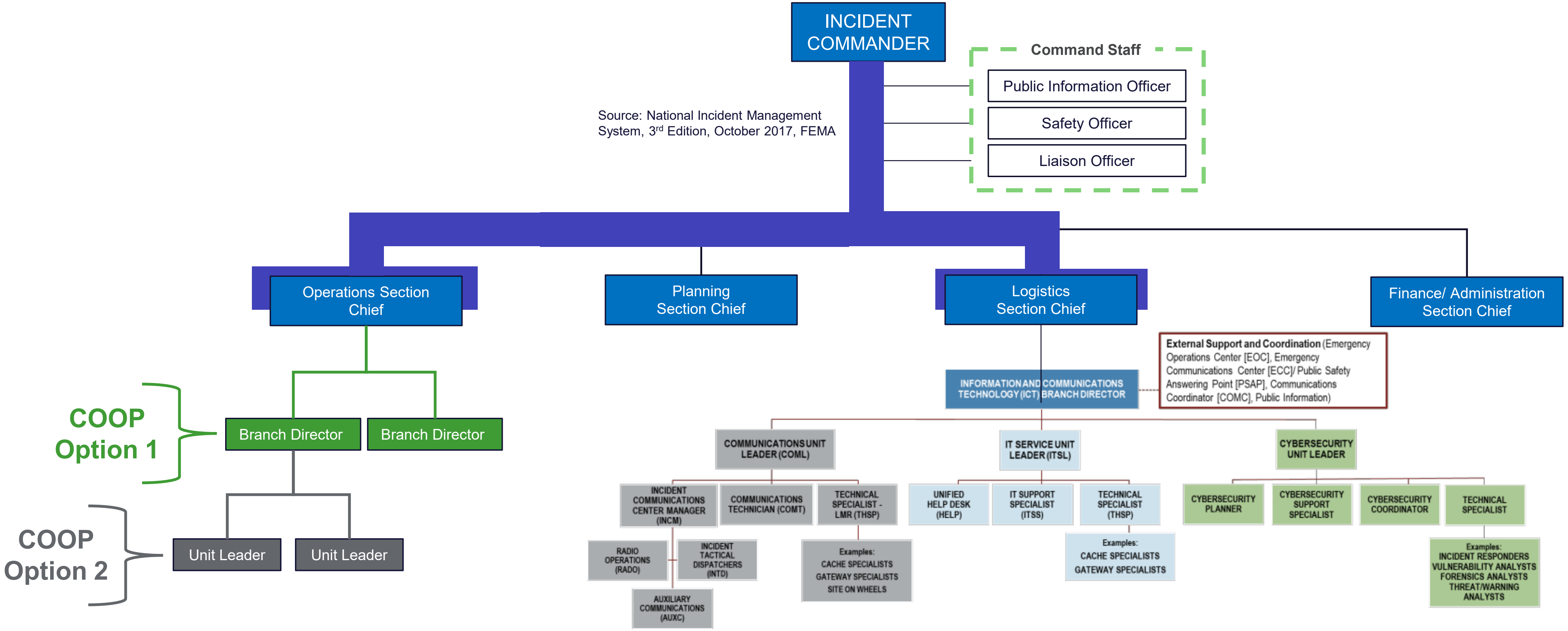
Best practice is to do Reconstitution planning during PMEF and MEF transition planning during Readiness.

Communication

Reconstitution

- Alternate Location Site Break-Down
  - Communication
  - Staff Transition
  - Site Breakdown

- Return to Daily Operations
- After Action Reporting



COOP and DR plans are <u>de-activated</u> by their respective branch directors in coordination with the Operations and Logistics Section Chiefs.

Reconstitution

- Alternate Location Site Break-Down
  - Communication
  - Staff Transition
  - Site Breakdown
- Return to Daily Operations
- After Action Reporting

Return to daily operations and After-Action Reporting

Reconstitution

AAR

All documentation (e.g., receipts, inventories, communication logs, briefing documents, etc.) should be collected by members of the Planning Branch.

De-mobilization

- Once the Incident Commander announces a return to daily operations, Reconstitution notifications are sent.
- The business and information technology infrastructure and resources and assets needed to stand-up the alternate location should be logged.
- All additional (or emergency) procurement should stop, and all receipts are collected and returned to the Finance Branch.
- Staff assigned to breakdown the alternate work location should review checklists and begin activities.

After-Action Reporting

- The timeline varies dramatically for each event on the after-action reporting process.
- Teams and Units should meet in their individual small groups to document observations and lessons learned.
- Eventually the after-action documentation will be submitted and coordinated across the Branches and the Sections for review and approval.
- A comprehensive After-Action Report should be included in the Integrated Preparedness Plan.

The same sequence to devolve non-mission essential functions should be followed to reconstitute them.

Case study

Case Study: Continuity of Operations

Client background

- State department of information technology contracted RSM for a wide-range of cyber security services
- COOP was included; however, state emergency management agency is the COOP lead.

The problem

- Emergency management and information technology lacked coordination
- Continuity planning mandated by the state and specifically led and coordinated by emergency management
- State agencies already began COOP
- Significant risk of duplicative efforts
- No plans to maintain PMEF and MEF during and following a *cyber event*
- Successful coordination needed to provide an operational plan
- Department of Information Technology lacked a Disaster Recovery Plan and exercise materials template for statewide deployment

Our solution

Collaborated with emergency management and information technology to develop and implement an operational non-technical cyber-COOP annex fostering cross-functional team collaboration:

- Agency partnership
  - Established a working partnership between the two state agencies focused solely on development of this COOP annex
  - Agencies committed to the collaboration to avoid duplication of efforts and align statewide planning to include disaster recovery planning
- Pilot agencies development and deployment
  - Four agencies (in addition to emergency management agency) agreed to participate in the development of this COOP annex
  - All agencies met individually and collectively with RSM to provide operational content and review and edit working drafts, which ensured alignment with statewide COOP and disaster recovery activities
- Pilot agencies workshop and exercise
  - Facilitated an in-person workshop to finalize a template of a Disaster Recovery Plan and a non-technical cyber event COOP annex
  - Facilitated a 6-agency tabletop exercise to test the disaster recovery plan template and COOP annex using the comprehensive exercise toolkit materials developed as part of the project activities
- Deployment statewide
  - Non-technical cyber-COOP annex
  - Disaster Recovery Plan template
  - Comprehensive exercise toolkit (disaster recovery and cyber security) aligned to FEMA HSEEP (Homeland Security Exercise and Evaluation Program)

Result

6

State pilot agencies with statewide implementation mandate for all agencies

Event disruption

Collaborated with pilot agencies on real event disruption to design immediate continuity and disaster recovery plans

Resiliency

Cross-functional collaboration on COOP and disaster recovery that enhanced resiliency

Questions

Thank you