

Mission Assurance Beyond the Basics

How investing in a mature mission assurance capability can transform a Department of Defense organization from compliant to truly resilient

June 2023

Introduction

Department of Defense (DoD) offices and agencies may be feeling content with their organization’s perceived ability to “build the plane while flying” – to execute basic principles of mission assurance (MA) and continuity planning while simultaneously shifting everything needed to perform day-to-day operations. After scrambling to write plans for mass telework, alternate work site logistics, and metered reconstitution, organizations may feel their plan for operating in a pandemic will facilitate mission resilience to whatever the next disruption may be. “If we made it through COVID,” the logic goes, “then we can get through anything.” But if this the logic, should the question instead be “how well did we actually do in response to COVID, whether we would do it the same way next time, and whether we truly believe there can be no greater threat to operations than a public health crisis.” With upcoming updates to the Federal Continuity guidance that create critical intersections with approaches to DoD MA programs and activities, the DoD and its constituent parts will need to reexamine how they build resilience throughout their operations in the future while integrating lessons from its past experiences.

Much of the vulnerability exposed by organizations’ response to the pandemic can be attributed to fragmented planning. Some organizations had emergency management plans, contingency plans, or portions of continuity plans. Few had pandemic plans. Some organizations wrote those plans on the spot and as a reaction to sudden circumstances but still maintained them in silos. To meet the **2022 National Defense Strategy’s**¹ fourth top priority—“build a resilience Joint force and defense ecosystem”—organizations will not only need to have these plans written, signed, and tested, but coordinated through an **Integrated Preparedness Plan (IPP)** to achieve a comprehensive resilience solution. An IPP lays out how plans such as those in Figure 1² actually *relate* to each other in execution (e.g., delineating where one stops and the other starts, and how organizations will train and exercise them together to create a full spectrum of resilience against all threats and hazards).



Figure 1 - DoD Planning Requirements with Related MA Benchmarks

¹ DoD, *2022 National Defense Strategy*, 27 OCT 2022. <https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF>

² From the Defense Threat Reduction Agency (DTRA)’s 2020 DoD MA Assessment Guidelines, signed 24 SEP 2020. Benchmarks in Figure 1 relate specifically to those with planning requirements. Acronyms: continuity of operations (COOP); cyber operations (CYBEROPS); chemical, biological radiological, nuclear, high-yield explosives (CBRNE); supporting material and services (SMS); force health protection (FHP); and emergency management (EM).

Aside from bringing MA plans under the governance umbrella of an IPP, organizations can make greater strides toward mission resilience through what its leaders do to **build on those individual plans and go beyond the basics**. Simply having plans written down may give leaders a false sense of security without advanced implementation targets, such as integrated risk management, threat and hazard monitoring technology, enterprise planning standards, realistic training and exercise, and planning coordination with mission partners.

This paper addresses how organizations can go beyond the basics of MA benchmarks by building the pillars of a mature MA capability shown in Figure 2. Given the evolving Federal continuity policy landscape, investing in advanced MA capability now can help organizations stay ahead of new requirements and build a more resilient defense ecosystem in the process.

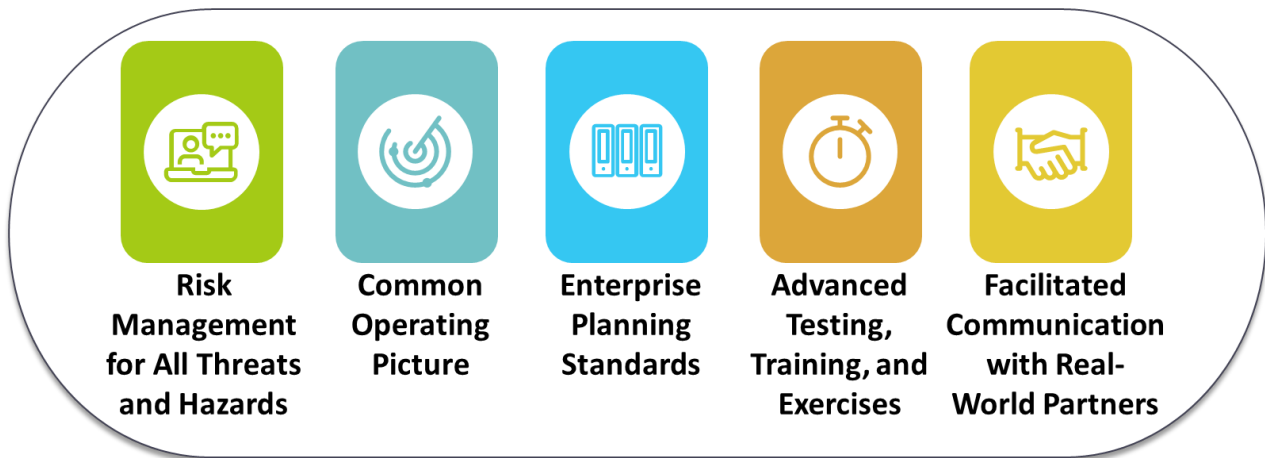


Figure 2 - Pillars of a Mature MA Capability, Deloitte Development LLC, Copyright 2023

Risk Management for All Threats and Hazards

“A comprehensive, integrated, and well-understood risk assessment methodology and process is at the heart of the mission assurance concept.” – DoD Mission Assurance Strategy³

Understanding the wide array of risks facing an organization and developing an approach to reduce those risks is a foundational element of MA. A full risk management process sets Federal government organizations up for effective implementation of resilience-building efforts by integrating risk management and continuity across all business functions. As such, a good risk management process integrates activities across multiple MA programs and activities to determine the likelihood and consequences of all threats and hazards to its essential assets, systems, and capabilities. This process should identify to what extent an organization’s mission essential functions (MEFs) might be impacted and guide planning for addressing those impacts to its operations. Mature risk management is an ongoing activity that involves assessing risks, understanding vulnerabilities, and identifying and implementing mitigation recommendations.

³ DoD, *Mission Assurance Strategy*, APR 2012.

<https://policy.defense.gov/Portals/11/Documents/MA Strategy Final 7May12.pdf>

An organization can start by establishing a risk management framework that defines a standardized process for the risk management approach. A mature MA construct involves repeatable risk management processes that can assess and manage risks across all program areas. The risk management framework should outline the scope of the assessment, the steps



Figure 3 - Deloitte's Risk Management Framework, Deloitte Development LLC, Copyright 2023

of the process, and the sort of data required to apply the processes to all essential assets, systems, and capabilities across the organization. DoD organizations can lay the foundation for this process by integrating guidance from DoD policies and manuals with industry leading practices from organizations such as the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO) to create a full risk management framework. Figure 3 below is an example of how risk management emphasizes continuity through alignment to essential assets, systems, and capabilities.

A component of effectiveness is the integration of risk assessment methodologies and the inclusion of external dependencies and interdependencies within the assessment process to understand the risks to the elements required for the execution of MEFs and the impacts of failure to manage risk both internally and with external partners. A standardized approach can enable an equivalent baseline understanding of risk across the organization and a means to monitor future risk management activities.

Following guidance within DoDI 3020.45 "Mission Assurance Construct,"⁴ organizations should have processes in place to conduct assessments at the local level to identify threats and hazards to assets and systems required to performance of MEFs as well as vulnerabilities related to those identified threats and hazards. Together, these aspects will define the risk to

⁴ DoD Instruction (DoDI) 3020.15, *Mission Assurance Construct*, signed 14 AUG 2018, change 1 02 MAY 2022. <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/302045p.pdf>

mission faced by each MEF and set a baseline for required risk management. The information on threats, hazards, vulnerabilities, and risks generated through this process will be critical to establishing a common operating picture for the organization as well as informing realistic training and exercise scenarios within the mature MA program.

A full risk assessment is merely the first step in the risk management process, allowing an organization to understand the risks to its operations at a global and local level. The goal of the organization should be a risk management program that identifies and implements measures to address those risks. Per DoDI 3020.45⁵, “DoD implements risk management by building redundancy, improving the day-to-day resilience of essential capabilities, or identifying the means to restore essential capabilities promptly after a debilitating event occurs.” DoD agencies should apply objectives-based planning processes to mitigation planning, identifying clear goals for mitigation activities tied to metrics that the organization can monitor for progress during implementation. Mitigation planning and implementation are critical elements to the DoD risk management process but cannot be performed in a vacuum. Organizations should coordinate mitigation measures closely with external partners to facilitate increased resilience against risks that stem from external assets.

While the effectiveness of mitigation may be often difficult to measure, continuous assessment cycles help an organization understand how its risk management process is improving its organizational resilience by highlighting immediate short-term improvements in addition to long-term resilience-building behaviors.

Common Operating Picture

“The goal of a common operating picture is to provide consistent, standardized, and geospatially-referenced information to the command, headquarters, and partner agencies.” – DoD Mission Assurance Benchmark EM-16, derived from DoD Instruction (DoDI) 6055.17.⁶

What elevates simple risk *awareness* to full spectrum risk *management* is an ability to see how and where risks may impact an organization’s assets⁷—the physical entities an organization uses to perform its MEFs—to guide responsive planning and prioritization of mitigation activities. Having a record of these task critical assets⁸ enables planners to begin connecting risks to real-world impacts and to plan mitigations through a combination of factors related to

⁵ DoD Instruction (DoDI) 3020.15, *Mission Assurance Construct*, signed 14 AUG 2018, change 1 02 MAY 2022.

<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/302045p.pdf>

⁶ DoD Instruction (DoDI) 6055.17, *DoD Fire & Emergency Services (F&ES) Program*, signed 03 OCT 2019.

<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/605506p.pdf>

⁷ DoD Directive (DoDD) 3020.40 defines “asset” as “a distinguishable entity... people, physical entities, or information that provide a service or capability.” DoD Instruction (DoDI) 3020.45 defines “asset owner” as the DoD component or subcomponent with planning, programming, budgetary, and execution (PPBE) responsibility for an asset.” These are distinct from “mission owners,” who rely on assets to execute a DoD mission.

⁸ DoDD 3020.40 defines these as assets of “such extraordinary importance [their] incapacitation or destruction would have a serious, debilitating effect on the ability of one or more DoD Components to execute the capability or mission-essential task [they] support.”

risk level and criticality. However, many basic MA capabilities keep these records of critical assets buried among other files and have no way to *visualize* those assets geospatially, much less in the context of real-time threats or hazards. A result is that many MA managers rightly claim to know what assets are critical to mission, but they cannot turn that information into action when needed, which turns risk mitigation into a perpetual state of catch up.

Going beyond the basics means being able to see the nexus between critical assets and threats in real-time. A common operating picture, while a staple of many mature operations center, is not a tool solely for emergency managers. MA stakeholders should also have access to such a capability for many reasons. A continuity event⁹ occurs when an organization's MEF, via disruption to a critical asset, is suspended for a period in excess of its maximum tolerable downtime (MTD). MA stakeholders need to know the moment such an event happens and have the tools to respond at their fingertips. **A mature MA capability has instant access to a common operating picture that overlays the organization's critical assets against threats and hazards, both historic and real-time.**

Common operating picture software on the market today provides continuity managers more than just real-time awareness of threshold events. It can automate triggers, send alerts, inventory resources, deploy relevant sections of digitized plans to task owners, and **account for personnel, even in transit or on temporary duty outside home station.** Today's software has mobile functionality, custom credentialing and access controls, and authorities to operate to host sensitive government data, even classified information. This capability can free up a continuity manager to focus on the human aspects of MA like quality control, stakeholder outreach, and leadership briefs.



Figure 4 - Sample Common Operating Picture – Virtual Command Center, Everbridge, Copyright 2021

Off-the-shelf common operating pictures can instantly take a continuity program beyond the basics but integrating **specific threat intelligence** like **commercially enabled intelligence or insider threat indicators** into the common operating picture's historic data can better equip organizations to stay ahead of **continuity events caused by malicious activity, not just natural disasters.** Software with an open application programming interface can ingest structured data

⁹ The only definition for “continuity event” in Federal doctrine comes from Department of Energy Order (DoEO) 150.1B, where it is defined as “an emergency caused by natural disasters, accident, military or terrorist attack, technological emergency, and infectious disease/pandemic influenza threat, which impacts or has the potential to impact the performance of **essential functions.**” Though DoD does not define “continuity event,” DoDI 3020.42 states “**performance of MEF** in a continuity event shall be the basis for continuity planning, preparation, and execution.” Bold added to the originals.

sets to produce an insightful overlay of threats or hazards, allowing continuity managers to forecast events that could have otherwise been invisible until the moment of impact.

Enterprise Mission Assurance Planning Standards

“Only with a coordinated, organization-wide approach can organizations ensure resilience and the ability to continue to perform essential functions during both catastrophic emergencies and routine disruptions both planned and unplanned.” – Federal Continuity Directive 2 (FCD-2)¹⁰

An IPP sets the foundation for cohesive planning, training, and exercise across an organization. An MA IPP outlines a coordinated timeline for reviews and updates of plans that serve as the basis for MA programs and activities. As organizations begin planning across the many MA programs and activities, they are often overwhelmed by the challenge of bringing an enterprise up to a uniform standard for each of these plans.

Organizations should establish a systematic approach to identify planning gaps, establish enterprise standards, and then **align development of their plans to their MEF(s)**, not their individual locations nor their enterprise as a whole. For large and dispersed organizations, this scoping makes the task more manageable – their daunting number of locations and personnel are non-factors for MA planning purposes; it is the number of MEFs they perform that matters. The challenge, then, falls to MA managers at the headquarters level who can set and enforce a series of **enterprise MA planning standards** without commandeering a process more effectively performed by those who actually perform the MEF at the local level.

The National Incident Management System is based on the belief all incidents begin and end locally. In terms of a dispersed enterprise, the locations where MEFs are performed are where each plan is activated, executed, and terminated. For a dispersed enterprise, the role of the headquarters MA manager is to keep “eyes on but hands off.”¹¹ A mature set of MA programs and activities **assigns planning responsibilities as closely as possible to the people who will actually be activating and operating their MEF at the local level**. This does not mean leaving those program officers to their own devices, but rather enabling them to combine their singular knowledge of a MEF with the organization’s planning standards for sustaining the MEF. The goal, after all, is to generate a cultural change where the whole organization sees MA planning as an act of resilience, not of compliance. Organizations looking to go beyond the basics should

¹⁰ Federal Emergency Management Agency (FEMA), “Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process,” *Federal Continuity Directive 2*, issued 13 JUN 2017. https://www.fema.gov/sites/default/files/2020-07/Federal_Continuity_Directive-2_June132017.pdf

¹¹ From Stanley McChrystal, LTG (Ret), in “Team of Teams: New Rules of Engagement for a Complex World.” The full quote, applicable here, is: “The temptation to lead as a chess master, controlling each move of the organization, must give way to an approach as a gardener, enabling rather than directing. A gardening approach to leadership is anything but passive. The leader acts as an “Eyes-On, Hands-Off” enabler who creates and maintains an ecosystem in which the organization operates.”

consider the following steps as a good approach to achieving uniform and high standards for an enterprise:

1. Create a headquarters-managed IPP to establish requirements for what MA-related plans are needed and at which levels of the organization these plans should reside
2. Identify and prioritize planning gaps identified within the IPP, outlining a timeline for plan development to help the organization address policy-driven planning requirements in an achievable, phased manner
3. For each individual planning requirement, create a headquarters “base plan” that addresses common organizational requirements and leadership functions that meet planning standards established in doctrine such as DoDI 3020.42 and forthcoming FCD updates
4. Establish policy associated with each individual planning requirement that outlines what each organizational subcomponent is responsible for with regard to local plans
5. Facilitate planning at the local level by socializing the base plan and providing associated templates that meet the enterprise planning standard outlined in policy
6. Align each plan with test, training, and exercise within the IPP to create a cohesive, enterprise approach to preparedness

Advanced Testing, Training, and Exercises (TT&E)

“Organizations should use TT&E to validate continuity plans, policies, procedures, systems, and alternate locations. Ensure corrective actions identified in exercises are tracked to completion.”
– DoD Mission Assurance Benchmark COOP-08,¹² derived from DoD Directive (DoDD) 3020.26¹³

Basic MA capabilities have no difficulty conducting testing, training, and exercises with enough regularity and relevance to meet the benchmark above. MA managers realize the need to train stakeholders with roles to play in executing plans, and they typically sequence testing and exercises to confirm the knowledge imparted through training has sunk in. In short, they do many of the required things to check the boxes and achieve a minimum standard. But the templates they use are rigid, scenarios are not driven by training objectives, and experience is lackluster. Overall, a basic MA capability’s TT&E events come across as an obligation, not an opportunity, and the organization is rarely more ready for a continuity event than it was the day before.

A mature continuity program uses exercises to increase readiness, making stakeholders grapple with problems they are likely to face in the real world before they actually face them.
A simple way for continuity managers to transform the program’s TT&E events from obligatory

¹² From the Defense Threat Reduction Agency (DTRA)’s 2020 DoD MA Assessment Guidelines, signed 24 SEP 2020.

¹³ DoD Directive (DoDD) 3020.26, *DoD Continuity Policy*, signed 14 FEB 2018.

<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302026p.pdf>

to engaging is to start with the organization’s own risk register to find the applicable scenario backdrop (“conditions”) for exercises. The intersection of critical asset, threat, and vulnerability (i.e., “risk”)¹⁴ is a point specific to each organization, and the proportional convergence of those factors should be the levers continuity managers pull to create customized, challenging exercise conditions. A mature MA program with an established risk framework has the basis for realistic scenario-building based on a data-driven understanding and prioritization of threats and hazards to the organization’s mission.

As a continuity program matures beyond the basics, its exercises should graduate from comfortable tabletops to functional exercises and full-scale exercises. Figure 5 below is a depiction of how continuity exercises can evolve with the maturity of a program.

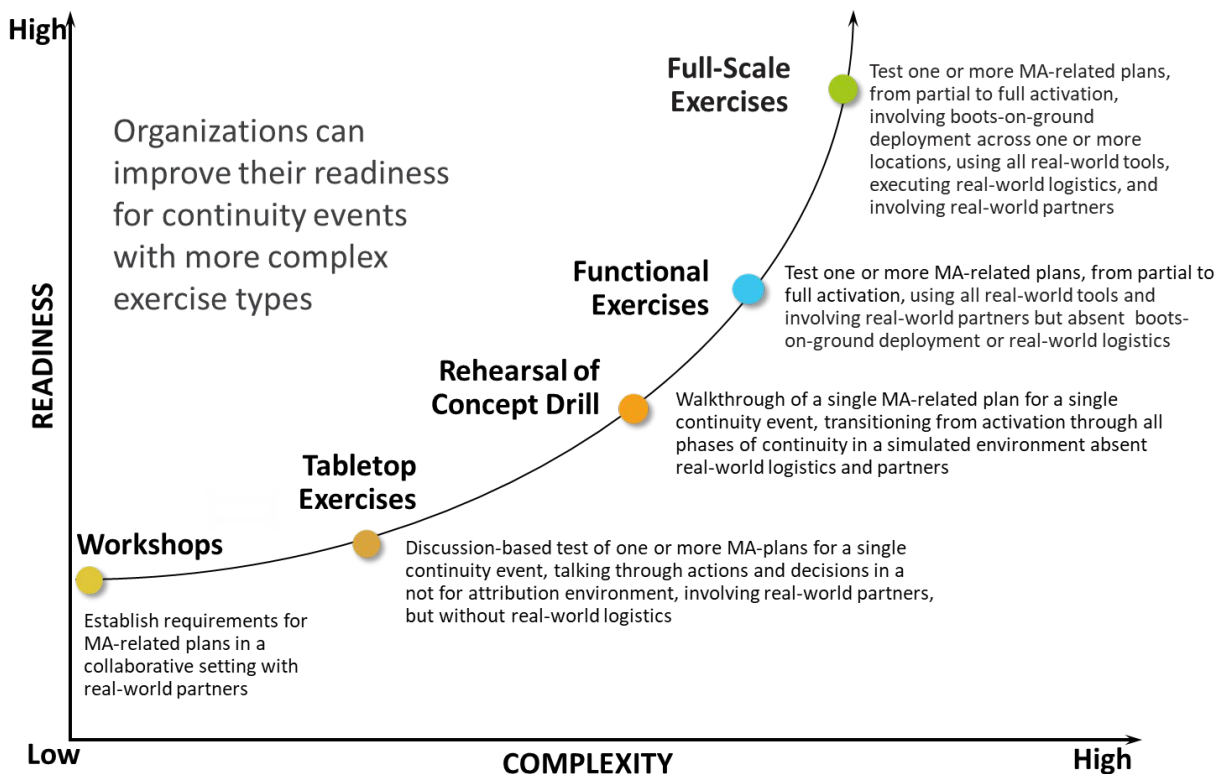


Figure 5 - Deloitte’s “Complexity Curve” for Resilience Exercises, Deloitte Development LLC, Copyright 2023

From workshops to full-scale exercises, **a mature continuity program exercises its stakeholders with appropriate realism and complexity for the organization’s next target state of readiness.** While an exercise should not prematurely test unwritten plans or untrained personnel, it also should not test the same plan the same way each time – that is a sign of a basic program and can be a cause of complacency. Exercises should involve the real players and partners, using real tools—common operating picture, emergency notification systems, communications systems, and other tools or technologies that stakeholders use to execute the plans being

¹⁴ These variables represent the three parts of the Defense Threat Reduction Agency (DTRA)’s definition of “risk” as it relates to mission assurance

tested—and they should encounter scenario conditions they will likely face in the real world, derived from the organization’s own risk assessment.

MA programs should record all TT&E events within the IPP, which is used to coordinate between planning and exercise, roadmap how exercises increase in complexity over time, and assess what level of real-world continuity readiness leadership can expect for their organization by taking corrective actions captured in After-Action Reports (AARs). Figure 6 at right shows the cycle that should be part of the overall IPP. Championed by leadership annually and maintained by the MA program, the TT&E elements of an IPP bring a sense of purpose to each event and helps participants “see the staircase” to an ever more capable MA program.

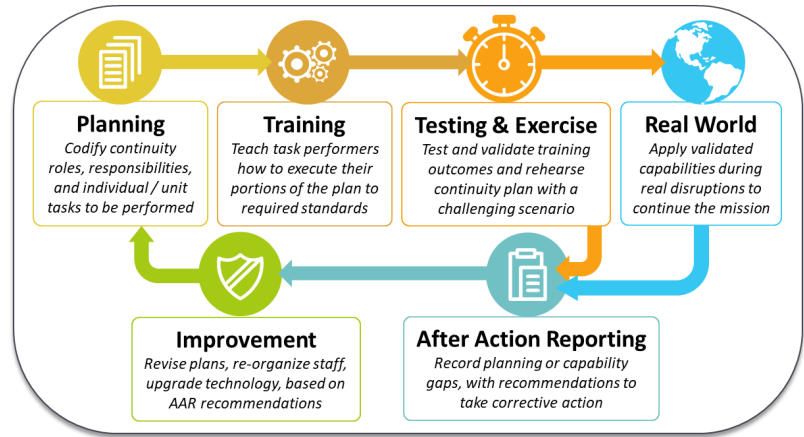


Figure 6 - TT&E Cycle with Sample Events for an IPP, Deloitte Development LLC, Copyright 2023

Facilitated Communication with Real-World Partners

“At many levels across DoD, ‘mission owners’ and ‘asset owners’ do not sufficiently coordinate or inform one another’s processes for assessing and mitigating mutual risk... DoD must nurture relationships and enhance information sharing with external stakeholders at each level of responsibility (installation, component, and DoD-wide).” – DoD Mission Assurance Strategy¹⁵

The complexity of DoD’s ecosystem of mission owners, capability owners, and asset owners¹⁶ can make it difficult to pinpoint where an organization fits into the DoD mission and what its individual responsibilities to mitigate risks really are. Many DoD organizations are made up of diverse subcomponents (e.g., some are asset owners, mission owners, or capability providers). Smaller organizations may cleanly fit into a single category, but they are still part of a larger

¹⁵ DoD, *Mission Assurance Strategy*, APR 2012.

https://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf

¹⁶ “Mission owner” is defined as “the DoD component having responsibility for the execution of all, or part, of a mission assigned by statute or the Secretary of Defense.”

“Asset owner” is “the DoD component or subcomponent with planning, programming, budgetary, and execution (PPBE) responsibility for an asset.”

“Capability provider” is “a DoD component that furnish forces, materiel, and other assets or capabilities to a mission owner to execute a mission.”

Sources: DoD Directive (DoDD) 3020.40, *DoD Policy and Responsibilities for Critical Infrastructure*, signed 14 JAN 2010. <https://policy.defense.gov/Portals/11/Documents/hdasa/newsletters/302040p.pdf>

DoD Instruction (DoDI) 3020.15, *Mission Assurance Construct*, signed 14 AUG 2018, change 1 02 MAY 2022. <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/302045p.pdf>

chain of interdependencies. To achieve Pillar 4 of the DoD Mission Assurance Strategy, “Partnering to Reduce Risk,”¹⁷ every organization must train itself to see the system, and no organization is exempt from a responsibility to coordinate with its partners to reduce systemic risks.

A basic MA capability knows its organizational identity—mission owner, asset owner, capability provider—but may still struggle to explain who depends on the organization’s continuity and why. For example, an organization might know it is an asset owner and have a correct inventory of its critical assets, but it might not know which mission owners, plans, agreements, or mission essential tasks (METs) depend on its assets. **A mature MA capability knows exactly where it fits in and how to forge working relationships with its dependent partners to share the risk reduction burden.** The asset owner in the above example works with the mission owner to record specific dependencies on its assets and achieve a mutual understanding of what is inexecutable without those assets – a process continuity managers call a business impact analysis (BIA), pursuant to **FCD-2 Annex D.**¹⁸ In this case, an impactful BIA should result in the mission and asset owner collaborating to protect those assets from failure.

An organization that realizes its dependencies and inherent risks better understands the need to coordinate MA plans across its spectrum of dependent partners. When each partner in Figure 7 can activate, operate, reconstitute, and devolve its MEFs in concert with the others, the system’s overall inherent risk is greatly reduced.

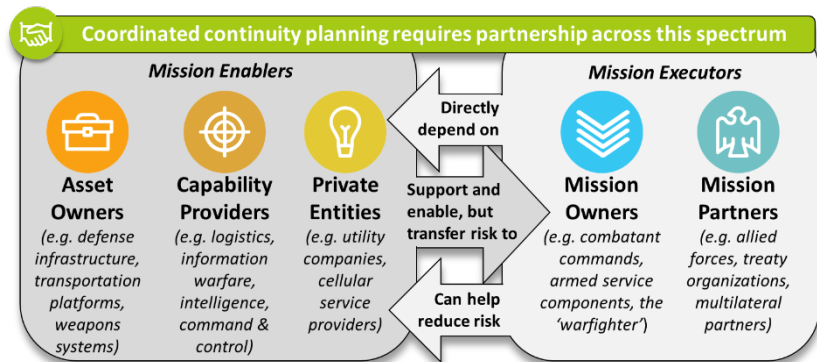


Figure 7 - Spectrum of Defense Ecosystem Partners, Deloitte Development LLC, Copyright 2023

But while it may sound obvious, getting to the table to actually coordinate continuity planning efforts with these stakeholders can be difficult and bureaucratic. A good place to start is with simple **stakeholder mapping to lay out priority stakeholders and visualize how these stakeholders interrelate.** This kind of documentation can tell leadership just how much they depend on, or are depended on by, a given stakeholder in the defense ecosystem. The results may be surprising or fairly obvious, but in either case, leaders will know which partners they should engage with first to address risks and how the nature and approach to those engagements should be designed.

¹⁷ DoD, *Mission Assurance Strategy*, APR 2012.

https://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf

¹⁸ FEMA, “Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process,” *Federal Continuity Directive 2*, issued 13 JUN 2017.

https://www.fema.gov/sites/default/files/2020-07/Federal_Continuity_Directive-2_June132017.pdf





Once an organization knows its priority interdependencies through stakeholder mapping, the next step is to achieve a **mutual, formal recognition** of those dependencies. Using official memoranda of understanding / agreement (**MOUs / MOAs**) or equivalents, interdependent organizations can consider the following acknowledgments, as a few examples:

- DoD installation or commercial facility hosts should recognize the “task critical” status of tenant assets and bring them into local continuity planning processes
- Mission owners should recognize the need to include continuity staff from asset owners and capability providers on which they depend in their own continuity plans
- Asset owners and capability providers should recognize priorities of mission owners in their continuity, contingency, or information technology disaster recovery (ITDR) plans
- Private infrastructure should prioritize restoration of service to DoD assets whose tolerable downtimes are the lowest, per mission owners, in emergency response plans
- Organizations should consider bringing the above stakeholders together on a recurring basis through a forum such as an MA Working Group

How Deloitte Can Help

Deloitte is currently supporting the National Continuity Program under the Federal Emergency Management Agency. As such, **Deloitte is the primary consulting professional service provider shaping the upcoming FCD updates, which establishes continuity planning guidelines for Federal departments and agencies.** Our access means Deloitte brings the latest knowledge of Federal continuity trends, long-term strategic shifts, and tactical requirements to help DoD organizations stay on the cutting edge of the industry.

To supplement knowledge of the latest in Federal continuity requirements, Deloitte brings additional service offerings to help DoD organizations **achieve advanced implementation targets for continuity** such as those described in this paper. See Table 1 below for a list of Deloitte’s offerings, tools, and sample deliverables to take DoD agencies beyond the basics.

Deloitte’s capabilities to provide the services in this paper			
Offering	Approaches and Knowledge	Tools	Outputs
Crisis & Resilience 	Full Lifecycle Emergency Management, MA Strategy, Risk Management, Integrated Preparedness Planning, Crisis Management Technology, TT&E, and COOP Staff Augmentation	Deloitte’s Resilience Framework, Policy and Plan Templates, Continuity Readiness Assessment tool, TT&E Handbook	Risk Register; Integrated Preparedness Plan, comprising COOP, ISCP, ITDR, Hazard Mitigation, EM/Emergency Action, and TT&E Plans; SOPs/Operating Instructions
Strategy & Operations 	Facilitated Communications with DoD Stakeholders; MA Program Development through Governance, Billeting, and Strategic Communication	Concept of Operations (CONOPS) Frameworks, Stakeholder Matrices; Modeling and Simulation Tools for Exercises	Watch Center CONOPS, MOUs/MOAs, Stakeholder Mapping; Tabletop Exercise Scenarios and After-Action Reports
Forensic Analytics 	Commercially-enabled Intelligence; Insider Threat Framework; Common Operating Picture Development	CEI Data and Analysis, Insider Threat Program Framework; Supply Chain Resilience tools (CentralSight™)	Threat Working Group CONOPS tied to Common Operating Picture (COP); CEI and Intelligence Data Sets, Daily Analytical Reports/ Situation Reports (SITREPs)
Industry Partners 	Critical Event Management Software, Crisis Technology, and Proprietary Intelligence Data Sets	COP Software; Emergency Mass Notification & Personnel Accountability Tools	COP and Emergency Mass Notification Technology with Select Customizations; Secure Access Controls

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2023 Deloitte Development LLC. All rights reserved.

Alex Haseley
Principal

Deloitte & Touche LLP
Tel: +1 202 329 4912
Email: ahaseley@deloitte.com

Elizabeth Nathaniel
Specialist Master

Deloitte & Touche LLP
Tel: +1 202 868 7612
Email: enathaniel@deloitte.com

Charlie Mink
Manager

Deloitte & Touche LLP
Tel: +1 202 236 6808
Email: chmink@deloitte.com