



UNITED STATES MARINE CORPS

MARINE FORCES RESERVE
MARINE FORCES NORTH
2000 OPELOUSAS AVENUE
NEW ORLEANS, LA 70114-1500

ForO 3058.1
G-3/5
12 Nov 2015

FORCE ORDER 3058.1

From: Commander
To: Distribution List

Subj: MARINE FORCES RESERVE (MARFORRES) MISSION ASSURANCE

Ref: (a) MCO 3058.1, "Marine Corps Mission Assurance Program",
October 23, 2014
(b) Mission Assurance Assessment (MAA) Stand Alone
Facility Benchmarks, February 17, 2015
(c) Mission Assurance Program Executive Committee Charter
(MAPEC), September 19, 2012
(d) MCO 5530.14A, "Marine Corps Physical Security
Program," June 05, 2009
(e) Operations Order 15-01, "U.S. Marine Corps Forces
North Mission Assurance", June 15, 2015
(f) NAVMC 3500.103, "Marine Corps Antiterrorism (AT)
Manual" October 27, 2010
(g) DoDD 4500.54G, "DoD Foreign Clearance Guide", December
28, 2009
(h) DTG 021526Z DEC 14, Marine Forces Reserve
Foreign/OCONUS Travel Requirements

Encl: (1) Mission Assurance (MA) Program Requirements/Risk
Management Methodology
(2) Marine Corps Mission Assurance - Enterprise Risk
Management
(3) Acronyms and Glossary

1. Situation

a. Purpose. This Order provides guidance for planning, implementation, and execution of the MARFORRES Mission Assurance (MA) procedures supporting the force protection and anti-terrorism programs at Reserve Training Centers (RTCs) across the United States and Puerto Rico.

b. Background

(1) MARFORRES operates in a decentralized environment with subordinate units in 46 states and Puerto Rico. Force protection and anti-terrorism measures vary from site to site as a result of local agreements and relationships with other Services, local law enforcements and Marine Corps Installations. This decentralization

DISTRIBUTION STATEMENT A: Approved for public release, distribution is unlimited

requires a comprehensive, synchronized MA program to protect against a number of potential adversaries with the ability to asymmetrically affect MARFORRES' ability to provide forces to augment and reinforce the active component.

(2) MA is a comprehensive approach that integrates all related protection and security activities and processes to the function of Risk Management (RM). MA encompasses all security functions within MARFORRES, to include: (1) antiterrorism (AT); (2) force protection (FP); (3) critical infrastructure protection (CIP); (4) continuity of operations (COOP); (5) physical security (PS); (6) operational security (OPSEC); (7) chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE); (8) emergency management (EM); (9) foreign disclosure program; and (10) foreign travel program. MARFORRES MA RM program activities assess and develop plans to manage risk as an integrated part of the Marine Corps planning process. Per reference (a), MARFORRES manages the MA program using standards contained in the Marine Corps MA Benchmarks per reference (b).

c. Applicability. This Order is applicable to all MARFORRES installations, RTCs facilities, and Marines, Sailors, and Department of Defense (DOD) civilians employed in the support of Commander, MARFORRES (COMMARFORRES) area of responsibility (AOR). Nothing in this Order shall detract from, nor be construed to conflict with the inherent responsibility of military Commanders to protect personnel and equipment under their command.

2. Cancellation. Force Order 3300.1.

3. Mission. MARFORRES establishes a MA Program to identify, assess, and manage risks to MARFORRES missions to man, train, equip, mobilize, and deploy forces in order to augment, reinforce, and sustain the active component (AC) with trained units and individual Marines.

4. Execution

a. Concept of Operations

(1) MA is intended to achieve a consistent, enterprise approach to RM and synchronize protection-related programs to adequately protect personnel, facilities, installations, equipment, information and information systems, supporting infrastructure, and logistic chains to preserve the capability to generate forces to augment, reinforce, and sustain the active component.

(2) Using this approach, plans are developed, trade-offs are weighed, and resources are invested based on a common risk picture and risk-informed decisions made by leaders at all levels across the Force.

(3) Consistent with the Headquarters Marine Corps MA Program, reference (a), MARFORRES' approach to MA implementation is based upon the following pillars:

(a) Increase Collaboration and Synchronize Policies, Tools, Information Sharing Mechanisms, and Investments across Protection-Related Programs. This pillar emphasizes closer coordination and enhanced information sharing between "mission owners" and "asset owners," as well as increased synchronization and integration of protection-related programs. MARFORRES MA Program's Office of Primary Responsibility (OPR) is the Assistant Chief of Staff (AC/S) G-3/5. To facilitate coordination, MA advocacy forums will be implemented to include the MARFORRES MA Program Executive Committee (MAPEC) per reference (c) and the MARFORRES MA Working Group (MAWG) which shall be established Force-wide starting at the local RTCs. Additionally, a Threat Working Group will be formed as an ad hoc action officer group designed to discuss current threats in the AOR and potential changes to Force Protection Conditions (FPCONs). These forums shall comprise a diverse mix of asset owners, mission owners, protection program subject matter experts, non-DoD supporting infrastructure and service providers, and civilian first responder organizations, as appropriate. This advocacy structure shall provide both local commanders and Inspector-Instructors (I-Is) as well as senior leaders the opportunity to assess and make informed decisions regarding risk, capabilities, gaps, supporting programs, and resource priorities.

(b) Implement a Comprehensive, Integrated All-Threats/All-Hazards MA RM Methodology and Process. A comprehensive, integrated, and well-understood RM methodology and process is essential to protecting the force, effectively executing MARFORRES missions, and achieving efficiencies across individual protection programs and activities. Enclosure (1) outlines the methodology and process that will unify the Force-wide approach to RM, including standardized assessment benchmarks and terminology. Use of this methodology and process will enable the examination of risk from an enterprise perspective and help identify risk trends and issues that individual commanders may not recognize or be able to manage adequately at their level. It will also facilitate the sharing of best practices and integrated approaches to RM across functional domains, programs, and asset types, and encourage continuous innovation as threats and vulnerabilities change over time.

(c) Risk-Informed Decision Making through an Enterprise MA Framework and Supporting Processes

1. An integrated, multi-level MA framework and supporting processes shall be established to enable the comprehensive assessment of risk; inform policy, plans, and resource allocation; and drive actions to manage risk effectively. Within this construct, many risk decisions will remain decentralized at the local command level.

Strategically, however, the MA framework and supporting processes will: Enable the management of risks that affect Force-wide mission performance; help determine Force priorities and economy-of-scale protection solutions; and provide risk-based inputs into the POM process.

2. MARFORRES will establish MA advocacy forums (MAPEC, MAWG, and TWG) that will be responsible for integrating outputs from the RA and gap analysis processes at their respective levels. They will also provide recommendations regarding protection capabilities, gaps, and priorities across individual program elements through their chain of command to the MARFORRES MA Division.

(d) Partner with External Entities to Further Identify, Assess, and Manage Risk to Marine Corps Missions. MA implementation will require extensive collaboration between MARFORRES, MCICOM and other DOD components and civilian government agencies. MARFORRES maintains sole ownership of 26 of its 161 sites. The remaining 135 sites are located on Marine Corps installations, installations of other Services or Joint Reserve Centers. These external partners have key authorities, capabilities, and resources that contribute to MARFORRES MA, both directly and indirectly. Hence, MARFORRES shall seek greater collaboration with these entities regarding joint risk and interdependent analysis, information sharing, scenario-based contingency and continuity of operations planning, all-hazards exercises, risk mitigation, and technological innovation.

b. Tasks

(1) AC/S, G-3/5

(a) Serve as the OPR for the MARFORRES MA Program.

(b) Serve as the chairperson of the MAPEC and hold semi-annual meetings to review issues presented by the MAWG and make appropriate recommendations to COMMARFORRES.

(c) Designate the chairperson of the MAWG and hold quarterly meetings. Present the results of the MAWG to the MAPEC to facilitate program direction and oversight.

(d) Designate a representative from the MA Division to participate in the Marine Forces North (MARFORNORTH) MAWG.

(e) Conduct annual all-threats/all-hazards protection exercises to ensure the integration of various protection-related requirements across the Force.

(f) Conduct annual program reviews of all Major Subordinate Commands (MSCs) with an on-site review conducted triennially to ensure compliance with program standards contained in

the MA benchmarks, to include Physical Security Surveys per reference (d), and provide action assistance as necessary.

(g) Ensure I-Is/Commanders conduct annual virtual program reviews via the MARFORRES MA Portal and triennially conduct a MA Assessment (MAA).

(h) Ensure U.S. Northern Command (USNORTHCOM) Force Protection Condition (FPCON) is disseminated and implemented by subordinate commands, to include the development of site-specific measures per reference (e).

(i) Monitor threat levels across the AOR and notify Higher Headquarters (HHQ) of deviations in FPCON.

(j) Designate a representative to participate in the Headquarters Marine Corps (HQMC) Security Division MA Operational Advisory Group (MAOAG) reference (a).

(k) Identify areas and assets that are vulnerable to attack and communicate these vulnerabilities via the Marine Corps Critical Asset Management System - Next Generation MCCAMS-NG) reference (a), (e), and (f).

(l) Coordinate AT Level II and Level IV training for the Force and maintain records of personnel trained and certified as ATOs.

(m) Collect and disseminate threat assessments and warnings to the Force.

(n) Collaborate and share threat information relative to mission critical assets and infrastructure with local, state, and federal authorities as required and within legal limits.

(o) Provide oversight on official and unofficial Outside Continental U.S. (OCONUS) travelers' compliance with the Foreign Clearance Guide, Travel Tracker/Individual Antiterrorism Travel Plan (TT/IATP), and APACS per references (g) and (h).

(p) Ensure Command Operations Center (COC) personnel are trained to monitor current threats, disseminate all-hazards threat information, as required, and execute Blue Dart Reporting.

(2) AC/S, G-1. Ensure 100% personnel fill for civilian and military billets in the G-3/5 MA Division and the COC.

(3) AC/S, G-2

(a) Disseminate Command threat/hazard assessments to the Force, as required.

(b) Develop and disseminate intelligence and counterintelligence products to support MA/AT/FP efforts.

(c) In conjunction with Naval Criminal Investigative Service (NCIS), monitor likely threats and hazards and report the same to the MAWG.

(4) AC/S G-4. Coordinate with the Director, Health Services, and Headquarters Marine Corps to ensure Command medical/health issues are identified to the MARFORRES MAWG.

(5) AC/S, G-6

(a) Maintain current status of Information Operations Conditions (INFOCON), web minimization, and operational directives in response to cyber-attacks.

(b) Incorporate MA into information sharing systems architecture to meet current DOD, Department of the Navy, and Marine Corps IA requirements.

(6) AC/S, Facilities

(a) Provide facility programming guidance concerning Uniform Facilities Criteria construction and repair requirements in support of MARFORRES MA Division.

(b) Be prepared to coordinate repairs/replacement to protective infrastructure that becomes damaged or destroyed.

(7) AC/S, G-7. Include MA Program Reviews with the MARFORRES Inspection Program.

(8) AC/S, G-8

(a) Identify and program resources for MA during the Planning, Programming, budgeting, and Execution Process.

(b) Ensure MA Division is adequately resourced with the appropriate structure to meet requirements across the Force.

(9) Public Affairs Officer. Provide public affairs guidance, provide press releases, and respond to media queries concerning consequence management and incident responses.

(10) Safety Director. Provide support and expertise on safety and risk mitigation issues for the planning and execution for the MARFORRES MA Division.

(11) Commanding Officer, Marine Corps Support Facility (MARCORSPTFAC) New Orleans

(a) Develop a comprehensive MA Program.

(b) In coordination with the MARFORRES and MARFORNORTH MA Director, ID, prioritize, and enter mission critical assets and supporting infrastructure into MCCAMS-NG.

(c) Conduct an annual MA Program Review of MARCORSPTFAC New Orleans and provide results to COMMARFORRES.

(d) Synchronize MARCORSPTFAC New Orleans MA plans with tenant plans during heightened FPCONS.

(12) Commanding Generals, 4th Marine Division, 4th Marine Aircraft Wing, 4th Marine Logistics Group, and Force Headquarters Group

(a) Develop a comprehensive MA program to identify, prioritize, assess, and manage risk; provide for remediation to mitigate vulnerabilities that could impact/degrade mission critical assets and infrastructure per reference (f).

(b) Develop and implement MA action sets/measures to be taken during each FPCON level. Ensure AT action sets are merged with all MA elements to include CIP and CBRNE.

(c) Identify an OPR for MA and appoint in writing personnel with responsibilities for AT, CBRNE, COOP, EM, OPSEC, and PS.

(d) Coordinate with MARFORRES MA to ensure MA program reviews are conducted triennially on subordinate units. Ensure subordinate unit Vulnerability Assessments (VA) are completed annually. Document discrepancies found during VAs on the MARFORRES MA Portal.

(e) Ensure subordinate units develop and execute RM processes for each element of the MA Program. All RM processes and procedures shall be reviewed at least annually per reference (a).

(f) Submit MA remediation/mitigation requirements utilizing the MA Portal FP Readiness Quarterly Report.

(g) Collaborate with local, State, and Federal authorities (within legal limits) regarding security issues relative to mission critical assets and infrastructure to maintain enhanced awareness.

(h) Partner with appropriate stakeholders to obtain risk-based protection solutions for the identified assets and infrastructure.

(i) For sites owned by MARFORRES, oversee development of a Training and Exercise Plan and conduct an annual MA exercise that encompasses RM methodology and security-related functions. Exercises shall include at a minimum AT, EM, CIP, and CBRNE scenarios as per references (a) and (e). For units that are tenants, ensure they participate in exercises on/in their bases, stations, installations, or facility (i.e., bomb threat, active shooter, COOP, EM event).

(j) Ensure subordinate units have documented and implemented COOP plans that provide the means to continue mission essential functions during all disruptive events.

(k) In collaboration with MARFORRES MA Division, ensure required MA training is conducted to include Level I through Level IV AT training. Manage Level II AT training requirements for site ATOs via the MARFORRES MA Portal.

(l) Ensure units are in compliance with USNORTHCOM designated FPCON and RAMs. Notify MARFORRES if required to increase the FPCON due to increased threat per reference (e).

(m) In coordination with the MARFORRES MA Division, ensure use of the MARFORRES MA Portal to disseminate FPCONS, intelligence, and indications and warnings to subordinate and adjacent units.

(n) Ensure subordinate units establish FP guidance for off-installation facilities, housing, and other activities used by or involving mass gathering of Marine Corps personnel, family members, and visitors.

(o) Designate points of contact for processing official and unofficial OCONUS travels in compliance with the FCG, TT/IATP, and APACs per references (g) and (h).

(p) Establish Memoranda of Understanding/Agreement with external entities as required to support MA and protection requirements.

(q) Submit waiver requests to COMMARFORRES via the chain of command, if implementation of MA requirements as outlined in this order and the references would adversely affect mission accomplishment submit waiver requests to Headquarter Marine Corps Physical Security per reference (d).

c. Coordinating Instructions

(1) All General and Special Staff, MSCs and CO, MARCORSPTFAC New Orleans designate personnel to participate in the MARFORRES led MAPEC, MAWG, and TWG to support an integrated MA Program.

(2) All General and Special Staff, MSCs and CO, MARCORSPTFAC New Orleans designate personnel to manage all official and unofficial travel to comply with Foreign Clearance Guide per references (g) and (h).

(3) Submit prioritized mission critical asset list to MARFORRES MA Division via the MARFORRES MA Portal no later than 10 September of each year per reference (f).

5. Administration and Logistics

a. Submit recommended changes to this order via the chain of command to the MARFORRES MA Division.

b. Reports. All reporting requirements and formats are contained on the MARFORRES MA Portal.

c. Logistics. None.

6. Command and Signal

a. The MARFORRES MA program is centrally managed by the OPR in the MA Division in the MARFORRES G-3/5.

b. Signal

(1) Primary communications for MA information sharing is through the MARFORRES MA Portal: <https://eis.usmc.mil/sites/mfrg3ma>

(2) Secondary means is via the MARFORRES COC:

(a) Telephone: DSN (312)647-7371; Commercial (504)697-7371.

(b) Email: NIPRNET MARFORRESCDO@usmc.mil; SIPRNET MARFORRESCDO@usmc.smil.mil.

c. This Order is effective on the date signed.


REX C. MCMILLIAN

DISTRIBUTION: C, D

Directives issued by this Headquarters are published and distributed electronically

**Mission Assurance (MA) Program Requirements/
Risk Management (RM) Methodology**

1. General. MA uses a risk-based framework to create synergies in implementing a standardized process for managing risk to the Operating Forces (OPFOR) and Supporting Establishment (SE) in the execution of their assigned missions, core functions, and related capabilities. MA also integrates and synchronizes numerous protection programs and other activities across the enterprise. This enclosure provides policy and procedures for a uniform, mission-focused, Risk Management (RM) process to be employed Marine Corps wide.

a. Goal. To develop and implement a uniform process for identifying and managing risk to assets that support the execution of Marine Corps mission and core functions/capabilities Service-wide. This mission-based approach also allows alignment and prioritization of effort across protection-related programs.

b. Risk Management (RM) Responsibilities. RM enables prioritization of protection capabilities and capability gaps, informs decision making, and provides for more focused resource allocation.

(1) Marine Corps Installations. Commanders execute RM as part of their annual MA process and supporting activities. Marine Corps tenant commands coordinate with and support the host installation's MA governance structure and supporting processes and associated RM activities. Under the joint basing concept, other service/agency tenants coordinate with and support the host installation's MA and RM processes.

(2) Operating Forces (OPFOR). Commanders execute RM as part of their operational planning per reference (d). RM principles are integrated into mission planning, preparation, and execution in all areas of operation. When OPFOR units are tenants aboard USMC installations, other service installations, or joint bases, OPFOR commanders will coordinate with and support their host installation's RM process.

(3) Marine Corps Security Augmentation Forces (SAFs). SAFs will conduct RM activities annually as part of the MA process.

(4) Assessments. Both higher headquarters (HHQ) and annual local assessments will utilize the most current Marine

Corps Mission Assurance Assessment (MCMAA) benchmarks, reference (f), and other approved directives when performing OPFOR, installation, facility, and asset assessments.

(a) Higher Headquarters Risk Assessments (HHQ RAs). All Marine Corps installations and OPFOR units that are tenants on installations will be subject to a MCMAA triennially. These assessments will focus on installation and tenant missions and associated critical assets, as well as applicable protection-related programs. Each assessment will evaluate the assessed command's RM execution, provide recommendations, and help advocate for improvement of the command's overall protection posture and those programs that support it.

(b) Annual Self-Assessment. Marine Expeditionary Force Major Subordinate Commands (MSCs) and installation commanders shall conduct risk assessments (RAs) annually, or more frequently if the threat/hazard (T/H) environment or mission requirements dictate. Commanders shall also conduct RAs for any event or activity deemed as a special event or which involves a gathering of 300 or more DoD personnel. DoD facility directives also require that a detailed RA be performed annually on utility systems. This self-assessment can be used to fulfill the annual requirement for utility systems identified as Supporting Infrastructure Critical Assets (SICAs) within the RA.

2. Risk Management. RM involves the application of a standardized process to identify, assess, and manage risk and enable decision making that balances risk and cost with mission benefits. RM allows the commander to decide how best to employ allocated resources to reduce risk, or, where circumstances warrant, acknowledge risk. As depicted in Figure 1, RM consists of two core activities, risk assessment and risk planning.

MCMAA Enterprise Risk Management Process



Figure 1 - MCMAA Risk Management Process

a. Risk Assessment (RA). An RA involves the collection and evaluation of data concerning asset criticality based on mission impacts, probable threats and hazards, and degree of vulnerability to determine the overall risk posture of the asset. An RA involves a systematic, rational, and defensible process for identifying, quantifying, and prioritizing risks. An RA involves the collection and evaluation of data in three core areas:

(1) Criticality Assessment (CA). A CA involves assessing the total impact (failure or severe degradation) on

the execution of missions or functions supported by an asset should that asset be unavailable for any reason. The CA identifies assets whose degradation or destruction impacts the command's ability to execute its assigned mission or functions. Commanders are required to conduct an annual CA utilizing the following process: 1) identify missions, functions, and associated standards and conditions for mission/function execution; 2) identify assets whose loss or unavailability will result in mission failure or severe degradation (mission impact).

(a) Mission Analysis. Mission Analysis provides the core foundation for conducting the CA. The overall objective of mission analysis is to gain an understanding of the missions that are being executed by a command, as well as how they are being executed. The output of this analysis will identify an inventory of assets associated with the execution of each mission or task assigned to a command. This asset inventory represents a starting point for the execution of the Critical Asset Identification Process (CAIP) to identify assets critical to mission execution. Mission analysis necessarily involves close coordination between tenant commands and host installations.

(b) Commander's Guidance. Commander's guidance is utilized to develop a mission statement, help understand the scope or parameters of required mission execution, and ultimately support the identification and prioritization of critical assets based on their impacts to supported missions. Utilizing command-approved Mission Essential Tasks (METs) or Mission Essential Functions (MEFs), together with their associated conditions, standards, and/or core functions, commanders will identify and validate assets that if degraded or unavailable for any reason would impact the command's ability to execute assigned missions, tasks, or functions. Assets can include personnel, equipment, facilities, information and information systems, infrastructure, and supply chains that support the execution of the command's mission and associated critical functions. The CAIP must be used to conduct the CA. In addition, there are other assets that may not be critical to the execution of the mission or function that may be identified during the criticality process and included in the overall RA. These could include assets such as theaters, commissaries, base exchanges, etc., that present significant issues related to force protection.

(c) Asset Identification. There are three major sub-processes involved in identifying critical and non-critical assets, all of which are outlined in the DoD CAIP. The first involves analysis of command-approved missions, tasks, and/or functions to identify Task Critical Assets (TCAs). The second involves analysis of each TCA to identify SICAs. The third involves the analysis of each SICA to identify any further SICAs, going at least one node beyond the facility. During this analysis, baseline elements of information (BEI) must be collected for each asset and entered into the Marine Corps Critical Asset Management System Next Generation (MC-CAMS NG) tool. Both DOD and the Marine Corps directed the use of the CAIP as the methodology to be used to identify two categories of assets - those that are critical to the execution of missions, tasks, and core functions, and those assets that are not critical, regardless of whether the asset is owned by the Marine Corps, other DOD components, other governmental entities, or the private sector.

(d) Asset Criticality Rating. Aligning one or more missions and related mission impacts to an asset will produce a criticality rating for that asset. This rating reflects an evaluation of the total mission impact an asset may have on all missions, tasks, and functions supported by that asset. This criticality rating is produced by use of either the Marine Corps Asset Prioritization Methodology (MC-APM) tool, or MC-CAMS NG when mission and mission impact data is populated in these tools (See paragraph 3, Risk Management Process and Tools, for a discussion of tools and supporting metrics). This asset criticality rating is also used as the CA rating in the Marine Corps Asset Risk Assessment (MC-ARA) methodology and tool. Along with Threat/Hazard (T/H) and Vulnerability ratings, the criticality rating contributes to producing a risk rating for an asset.

(2) All Hazards Threat Assessment (AHTA). Execution of the RM process is also based on an assessment of the threat and hazard environment in which Marine Corps forces and installations operate and missions are executed. The development of an AHTA will accomplish two goals: 1) identification of a comprehensive list of threats and hazards, and 2) identification of the likelihood or probability of occurrence of each threat or hazard. An AHTA must be executed annually, tailored to the local environment, and ensure all threat and hazard information is integrated to meet the command's effort to manage risk to missions, personnel, and assets. The AHTA also supports a consistent view of the T/H

environment to support Installation Emergency Management (IEM), Chemical, Biological, Radiological, Nuclear, and High-yield Explosive (CBRNE), Antiterrorism (AT), Critical Infrastructure Program (CIP), law enforcement (LE), Fire and Emergency Services (F&ES), 911 dispatch, physical security (PS), and continuity of operations (COOP) protection and response planning. A collaborative effort among the membership of the Mission Assurance Executive Councils (MAECs) and Mission Assurance Working Groups (MAWGs) representing the various protection-related programs (CBRNE, IEM, CIP, AT, PS, and LE) will be required to develop the AHTA. The AHTA is also based on the fusion of information (strategic, operational, and local tactical) derived from liaisons between civil and military LE; public safety agencies and departments; and meteorological, environmental, public health, and medical syndromic surveillance sources. In the context of assessing risk, the higher the probability or likelihood of a threat or hazard occurring, the higher the risk of loss will be to the asset - all other factors being equal. As part of the command RM process, commanders will develop an integrated and prioritized T/H matrix that reflects the likelihood of assessed threats and hazards (See Figure 2 - Individual Threat/Hazard Analysis Data Matrix).

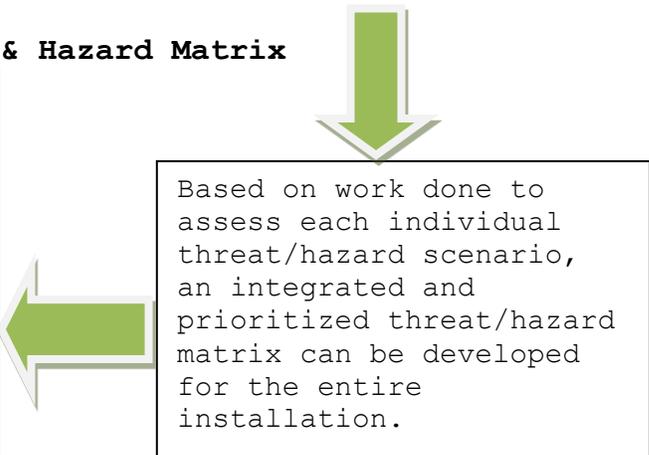
(a) Hazard and Threat Analysis. Analysis must be conducted to identify a T/H baseline that could adversely impact command assets¹ (See Figure 2 - Individual Threat/Hazard Analysis Data Matrix). The results of this annual AHTA analysis must be integrated into all aspects of the RM process.

¹ When discussing execution of Vulnerability Assessments (Vas) below, the assessor must align one or more identified threats/hazards to one or more vulnerabilities of assets or the installation that could be exploited by the threat or hazard.

Installation / Site Name	Threat / Hazard Name	T/H Probability Rating Ranges	Probability Rating Source Information	Assessed T/H Probability Rating	Other Rating Factors - Comments
Camp Zebra	Explosive - 220 lb. VBIED	Critical .76 to 1.00	NCIS Threat Assessment dated x/xx/xx; DIA Threat Assessment dated x/xx; Local installation threat assessment dated x/xx; past history of similar events occurring, etc.	HIGH .60	Site specific intelligence factors; other relevant analysis such as a DBT; identify a specific period for duration of the threat or hazard;
		HIGH .51 to .75			
		Medium 26 to .50			
		Low .01 to .25			

Integrated and Prioritized Threat & Hazard Matrix

Installation / Site Name	Threat / Hazard Name	Assessed T/H Probability Rating
Camp Zebra	Flooding - Hurricane	
	Explosive - 220 lb. VBIED	HIGH .60
	Aged Equipment - No Spares	Medium .47
	EMP	Low .05



Based on work done to assess each individual threat/hazard scenario, an integrated and prioritized threat/hazard matrix can be developed for the entire installation.

Figure 2 - Individual Threat/Hazard Analysis Data Matrix

(b) T/H Probability Ratings and Definitions. Once a baseline of threats and hazards has been identified, the assessor must conduct an analysis to determine the likelihood or probability of occurrence of each threat and hazard. There are four categories of T/H probability ratings: critical, high, medium, and low. The T/H probability ratings can be found in the MC-ARA standalone tool, located on the Headquarters Marine Corps (HQMC) PS division SharePoint portal: <https://ehqmc.usmc.mil/org/ppo/PS/PSM/MAAT/Shared%20Documents/Forms/AllItems.aspx>. T/H probability ratings and definitions are also embedded in MC-CAMS NG tool. The use of these ratings and definitions will facilitate the uniform assessment of the likelihood or probability of occurrence of any individual threat

or hazard. Probability is defined as the estimate of the likelihood that a threat will occur.

(c) Threat/Hazard Ratings:

1. Low (.01 to .25): Indicates little or no credible evidence of a threat to the asset or the immediate area where the asset is located.

a. For the identified threat, there is little or no credible evidence of capability or intent and no demonstrated history of occurrence against the asset or similar assets.

b. For the identified hazard, there is a rare history or no documented history of occurrence in the immediate area or region where the asset is located.

2. Medium (.26 to .50): Indicates a potential threat to the asset or the immediate area where the asset is located. Also indicates there is a significant capability with low or no current intent, which may change under specific conditions and low or no demonstrated history.

a. For the identified threat, there is some evidence of intent, little evidence of a current capability or history of occurrence, and some evidence that the threat could obtain the capability through alternate sources. Alternatively, the identified threat evidences a significant capability, but there is little evidence of current intent and little or no demonstrated history.

b. The identified hazard has a demonstrated history of occurring on an infrequent basis in the immediate area or region where the asset is located.

3. High (.51 to .75): Indicates a credible threat against the asset or the immediate area where the asset is located.

a. The identified threat has both the capability and intent, and there is a history that the asset or similar assets are, or have been targeted on an occasional basis.

b. The identified hazard has a demonstrated history of occurring on an occasional basis in the immediate area or region where the asset is located.

4. Critical (.76 -1.00): Indicates an imminent threat against the asset or the immediate area where the asset is located.

a. The identified threat has both the capability and intent and there is a history that the asset or similar assets are being targeted on a frequent or recurring basis.

b. The identified hazard has a demonstrated history of occurring on a frequent basis in the immediate area or region where the asset is located.

(d) Threat/Hazard (T/H) Categories:

1. Human-caused intentional threats include: insider threat, cyber, active shooter/lone offender, foreign intelligence entities (FIE), terrorism (including domestic terrorists, transnational terrorists, and terrorist use of CBRNE), crime (including non-violent crime, violent crime, gang activity, and narcotics), conventional/strategic military threats, and civil disturbance.

2. Hazards are broken down into three categories: Natural Hazards, Accidental, and Technologically-caused events. These sub-areas are further described below.

a. Natural Hazards: The Natural Hazards category includes Geological, Meteorological and Biological hazards. Geological categories include volcano, tsunami, earthquakes, and landslides. Meteorological categories include: hurricanes, tornado, drought, winter weather, fire, extreme heat, lightning, hail, wind, rain, and flooding. Biological categories include: diseases that impact humans or animals such as plague, smallpox, anthrax, West Nile virus, foot and mouth disease, severe acute respiratory syndrome (also known as SARS), pandemic disease, bovine spongiform encephalopathy, etc.

b. Accidental Events: Accidental events can cause disruption to the operation of assets, as well as the execution of missions supported by those assets. Accidental events can take many forms, from events that result from human error (man-made) to those accidental events that are caused by

technology or technological failures. Incidence ranges and frequency must align with the Hazard probability definitions (Low, Medium, High, and Critical) to determine the overall probability rating. Examples of various types of accidental events include, but are not limited to:

(1) Man-made accidental events such as construction accidents (e.g., a Back-hoe that unintentionally cuts a power, water, fuel, or communications line);

(2) Errors or mistakes in operating equipment or vehicles; mishaps such as inadvertent chemical spills; wildlife-induced accidental events, such as wildlife accessing and damaging assets (e.g., wildlife shorting out electrical transformers);

c. Technologically-Caused Events.

Technologically-caused accidental events include but are not limited to: aging assets and infrastructure that are past their normal life cycles and fail in some way; equipment failure caused by power surges or "dirty" power; equipment overheating (such as servers when the heating, ventilation and air conditioning (HVAC) system components fail); or software bugs that disrupt systems and networks. Statistics are gathered onsite at specific locations and generally are not available from national data bases.

(e) Sources of Threat Assessment Data. The MCMAA Program has established a detailed list of authoritative sources that support the development of the AHTA. The AHTA Methodology can be found on the HQMC Mission Assurance Assessment SharePoint portal: <https://ehqmc.usmc.mil/org/ppo/PS/PSM/MAAT/Shared%20Documents/Forms/AllItems.aspx>.

(3) Vulnerability Assessment (VA). The VA process involves identifying the characteristics of an asset that could cause it to suffer degradation or loss (incapacity to perform its designated function) as a result of having been subjected to one or more threats or hazards. A VA is a systematic examination of the characteristics of an installation's system, asset, application, or its dependencies to identify vulnerabilities that could be susceptible to the effects of any number of threats or hazards. VAs must be conducted by teams of subject matter experts with backgrounds in different functional areas such as PS, AT, CIP, Counterintelligence (CI), and installation integrated protection. VAs will be conducted as follows:

(a) Identify and assess all vulnerabilities to the installation, facilities, and assets, specifically including all identified critical assets. Vulnerability is defined as a weakness or susceptibility of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard effects. Vulnerabilities can result from a wide variety of factors such as: design and construction flaws, environmental factors, proximity to other structures or systems, factors influencing accessibility, personal behaviors of individuals working in or around the assets, or operational practices associated with the assets or the installation. Vulnerabilities can also be a function of vulnerabilities to other assets or areas that are not in close proximity to the asset. For instance, vulnerabilities in installation access or perimeter control may lead to an adversary gaining access to the installation, and ultimately to an asset located somewhere on site.

(b) Align specific threats and hazards to asset vulnerabilities. Threat-vulnerability pairing is conducted to link likely threats and hazards to specific asset vulnerabilities that may be susceptible to a specific threat or hazard. This process is crucial because individual assets may have a greater degree of vulnerability to different threats or hazards. Threat-vulnerability pairing, in turn, will support the preparation of effective risk reduction plans designed to lower overall risk by incorporating and addressing both threat/hazard and vulnerability analysis in those plans.

(c) Identify degrees of vulnerability. When assessing and identifying vulnerabilities, the assessor needs to make a judgment as to the significance or degree of an identified vulnerability. For example, lack of standoff around a high population building may be identified as vulnerability, based on Unified Facility Criteria (UFC) requiring 25 meters of standoff distance with an actual standoff distance of 24 meters. In this particular case, the significance or degree of vulnerability would be rated relatively low, as would the impact of exploiting that vulnerability from a threat such as a Vehicle Borne Improvised Explosive Device (VBIED) that the UFC requirement was designed to address. Identifying degree of vulnerability helps establish a vulnerability score, which, in turn, supports the establishment of an overall RA rating. Degrees of vulnerability are defined in the MC-ARA tool and MC-CAMS NG.

(d) Vulnerability Ratings Definitions

1. Low (.01- .25): Indicates multiple effective layers of integrated countermeasures in place and no known weaknesses through which adversaries, natural hazards, or accidental disruptions would be capable of causing loss of or disruption to asset.

2. Medium (.26 to .50): Indicates multiple effective countermeasures in place; however, at least one known weakness exists through which adversaries, natural hazards, or accidental disruption would be capable of causing loss of or disruption to asset.

3. High (.51 to .75): Indicates some effective countermeasures in place, but multiple known weaknesses exist through which adversaries, natural hazards, or accidental disruptions would be capable of causing loss of or disruption to asset.

4. Critical (.76 -1.00): Indicates minimal effective physical, design, technical, procedural, or behavioral countermeasures in place and many known weaknesses through which adversaries, natural hazards, or accidental disruptions would be capable of causing loss of or disruption to critical assets.

(4) Risk Rating. A risk rating is established based on the values produced from the Criticality Assessment (CA), AHTA, and VA. Risk is determined by the following equation: criticality rating x T/H rating x vulnerability rating = risk rating. MC-CAMS NG provides an integrated set of metrics to establish a risk rating. The risk rating is produced for each specific T/H and vulnerability/asset data pairing.

b. Risk Planning. The objective of the RM methodology is to enable the management of risk based on a holistic approach that cuts across individual programs and capabilities such as: AT, CIP, PS, CBRN, COOP, etc. Since some risk will always be present, RM seeks to achieve an acceptable level of risk in the execution of a command's missions and functions. The RA process seeks to evaluate and identify asset risk of loss based on an asset's criticality (mission impact), the probability of the occurrence of specific threats and hazards, and associated degrees of vulnerability. Risk planning is the process of determining options or courses of action (COAs) to reduce the risk of loss to the asset, and thus reduce impact to mission execution. To support the development of risk reduction plans,

commands can leverage elements of the MA governance process such as the MAECs and/or MAWGs, or establish a risk reduction planning team consisting of experienced personnel with necessary expertise. Risk reduction planning involves two areas of implementation: Risk Reduction Plan Development, and Acknowledgement of Risk:

(1) Risk Reduction Planning. Commanders will implement effective and efficient risk reduction COAs whenever possible. Examples include, but are not limited to, PS measures, personal protection measures, cyber security measures, and/or building redundancy in assets critical to mission execution, etc. Risk reduction planning COAs can involve efforts to implement risk reduction measures both before an event occurs that could adversely impact missions and assets (previously known as "remediation"), as well as measures that are implemented after an event, or after receipt of warning of an impending event (previously known as "mitigation").

(a) Risk Decision Packages (RDPs). RDPs represent one or more COAs designed to address and reduce identified risk to assets and missions. RDPs are developed to assist commanders in risk decision making. RDPs must be documented in MC-CAMS NG for all Tier I-III critical assets, at a minimum. The following elements must be included in a RDP:

1. Executive Summary
2. Mission Details
3. T/H Details
4. Asset/Vulnerability Details
5. Initial Risk Rating
6. Proposed risk reduction COA and the estimated reduction in risk anticipated.

(b) Cost Benefit Analysis. Proposed risk reduction COAs identified as part of any risk reduction plan should include a cost-benefit analysis. The following should be considered as part of this analysis:

1. Doctrine: Policy, procedures, guidance, and agreements with internal and external tenant commands/agencies

2. Organization: Structure and location
3. Training: Formal, informal, and situational
4. Material: Physical, cyber, financial resources, and redundancy
5. Leadership: Education, knowledge, and experience
6. Facilities: Physical, access, security, and resilience

(c) Analyze Options and Determine the Best Approach. This step focuses on analysis of one or more COAs to determine the option that represents the most "bang for the buck". Use of the MC-ARA tool or MC-CAMS NG will assist commanders in analyzing options and determining the best COAs to implement. Executive-level planning groups will include a cost-benefit analysis to balance risk to the asset and/or mission with the resource requirements necessary to reduce risk.

(d) Develop and Coordinate the Risk Reduction Plan. This step involves development of a Plan of Action and Milestones (POA&M) outlining details of what needs to be done, how it is to be done, who is involved, and the timeframe to complete implementation of the risk reduction plan. The plan must include details concerning the asset, specific T/H to which the asset is vulnerable, information concerning the command's decision to reduce risk, and resource requirements needed to execute the plan.

(e) Implement the Risk Reduction Plan. This step follows plan approval and involves the tracking of the milestones developed in the above POA&M and the measurement of success in reducing risk previously identified. Plan effectiveness is assessed through the command's annual exercise program or through higher headquarters RA, such as a MCMAA.

(2) Acknowledgement of Risk. Commanders have several options in weighing risk. Risk can be acknowledged, locally funded, or reduced by implementing remediation measures to reduce the risk, or the risk element can be forwarded to HHQ for funding or other consideration. A command may decide to "acknowledge risk" to assets where appropriate, rather than dedicating resources to reduce identified risk. Risk may be acknowledged by the command when the impact of loss or the

anticipated reduction in risk is not significant enough to justify the cost or the minimal benefit of the proposed risk reduction countermeasure. The command also may acknowledge risk temporarily where resources are not currently available to support desired risk reduction COAs. In these cases, documenting acknowledgement of risk in MC-CAMS NG is also the first step to be undertaken to identify such risk up the chain of command.

(a) Higher Headquarters (HHQ) Risk-Informed Decision Making. Commanders should prioritize proposed risk reduction COAs that cannot be implemented at their level for current year or Program Objective Memorandum (POM) funding solutions. When effective and efficient countermeasures cannot be implemented immediately, commanders must prioritize any remaining risks to compete for funding solutions. HHQ risk-informed decision making involves a chain of command-driven process in which a risk-related unfunded resource requirement is submitted to HHQ for current year funding or via the Planning, Programming, Budgeting, and Execution (PPBE) process or the MA governance structure and supporting processes.

1. MCMA-E RM. MA personnel at all levels within the Marine Corps continuously update their RAs to alert the commander to emerging threats and associated vulnerabilities which need to be addressed. At the installation level, typical factors to consider in the development of risk reduction plans include, but are not limited to: physical security and access control, cyber security, personnel security, facility design, critical asset and infrastructure resilience and redundancy, emergency response planning and resourcing, and training and exercises (See Figure 1 for an outline of MCMA-E RM processes).

(b) Other Risk Reduction Planning and Coordination Considerations:

1. Capability Assessment. A Capability Assessment is a command or unit-level evaluation designed to identify capabilities for responding to an event, whether caused by intentional conduct or by a natural or unintentional manmade disaster or hazard. All installations shall conduct capability assessments and consider contingency planning activities. Planners should make full use of their Capability Assessment when developing COAs that will rely on the Command's response capabilities as an integral part of the risk reduction plan.

2. Confirm Stakeholders, Prioritize Risk, and Identify Options. It is important to identify asset owners, mission owners, and other stakeholders that have a vested interest in reducing risk to missions and assets. MC-ARA and/or MC-CAMS NG will be used to prioritize risk to assets, as well as to prioritize impact of critical assets on all the missions supported by the asset. These tools and processes generate priority values for impact to missions and the identification of risk. Risk reduction efforts will focus on obtaining optimal risk reduction and the most effective/efficient use of resources.

(c) Required Risk Reduction Plans. Risk reduction planning includes the development of the following plans that are typically implemented during or after an event, or upon receipt of warning of an impending event:²

1. Installation Emergency Response Priority Plans. This plan establishes first responder and other emergency response priorities with a focus on mission continuity once life-saving activities are executed.

2. Utility Restoration Priorities. This plan identifies the priority for restoring utility infrastructure (e.g., electricity, water). Priority of restoration should take into account restoration of utilities supporting critical asset operations. Priority restoration plans should be identified and integrated for critical assets supporting both installation and tenant commands.

3. Installation Security Response Priorities. These plans address actions taken in concert with T/H indications and warnings that necessitate an escalation in security response and/or security measures. Examples of these plans include the Security Force Augmentation Plan, Random AT Measures Implementation Plan, and FP Condition Action Sets Plan. Security response and protection measure priorities should be identified for locations housing critical assets, including those critical assets owned by tenant commands, within the overall host installation security response priority planning.

4. Continuity of Operations Plans. These plans integrate Marine Corps COOP requirements with existing protection policies and programs focused on the protection of critical resources and infrastructure and continuation of MEFs.

² All risk reduction plans must be documented in MC-CAMS NG.

5. Reconstitution Plans. These plans are developed in advance of an event to address the loss of critical assets that support installation and tenant command missions, tasks, and essential functions.

(3) Process Review. Assessing risk and conducting risk reduction planning is part of a continuous cycle. Although commands are required to assess risk annually, a command's missions, T/H, and vulnerabilities can change at any time. Risk should be re-evaluated as these changes occur.

(a) Updating Critical Asset Risk Profile/Rating. Update critical asset risk profiles/ratings annually or when changes in the criticality, T/H, or vulnerability occur. Significant increases in risk profiles/ratings may require changes in risk reduction plans or strategies and resource priorities.

(b) Program Review. Once the annual RM process is complete, it is essential to conduct a thorough review of the overall process. This is typically accomplished as part of the annual program review.

(c) Refine RM Plan. The RM process is executed in a cycle. Revisions to plans should be accomplished and documented to enable plan improvement.

(d) Coordinate with Stakeholders. Commanders should ensure that stakeholders in the military and local civilian communities are involved in the process review. This collaboration will ensure that supporting plans align with the RM process. Local community stakeholders can also help identify strengths and weaknesses, focusing on collaboration between military and civilian agencies. Complex operating environments magnify the importance of coordinating with Marine Expeditionary Forces and installations. In order for expeditionary commanders to effectively manage risk, those with protection responsibilities under their command should possess a solid understanding of the local customs, culture, and society in which they operate. Interfacing and coordinating preventive and/or response measures with local stakeholders will help ensure a more robust security and response posture. However, coordination with local stakeholders should never be done at the risk of endangering DoD personnel, assets or USMC missions.

(e) Exercise and Modify Risk Reduction Plans. The final stage in the RM process review involves the exercising of

risk reduction plans that have been implemented during annual exercises, and making adjustments as needed.

3. Risk Management Process and Tools. The following is a list of processes and tools required to be used in the execution of MCMA-E RM process.

a. MC-CAMS NG. MC-CAMS NG is a mission and asset risk management-focused data management system designed to provide operational and contingency planning support for multiple MA and RM tasks and requirements. MC-CAMS NG is used to enter risk management data, including RA and risk reduction planning results and information. MC-CAMS NG incorporates both MC-APM and MC-ARA methodologies. Where appropriate, MC-CAMS NG will automate the sharing of risk management data with other DoD Components and data management systems.

b. MC-APM. The MC-APM is a standardized, mission-focused methodology that supports prioritization of Marine Corps assets and infrastructures - both critical and non-critical. Prioritization is based solely on the following metrics related to the mission and its execution:

(1) Level of Task, Function or Capability (e.g., tactical level to strategic level);

(2) Mission Impact (Failure, Severe Degradation, or No Significant Impact);

(3) Time to Mission Impact (time from asset unavailability to the time mission is impacted);

(4) Time to Restore the Asset or its capability provided to the mission (assume asset is completely destroyed); and

(5) Elements (1)-(4) are captured for every mission, task, functions that the asset supports.

Each of these data elements must be captured and entered into MC-CAMS NG to enable the prioritization of assets. All identified assets will have their asset priority score determined by use of the MC-APM.³

³ Asset priority value is also the impact value or score that is utilized in the MC-ARA methodology and tool to support the determination of risk of loss to the critical asset.

c. MC-ARA. This stand-alone tool provides an integrated set of metrics and definitions that support a standardized process for the identification and analysis of criticality, T/H, and VA functions resulting in the production of a risk rating. These same risk assessment metrics and methodologies are also embedded in MC-CAMS NG. Each of the risk assessment data elements; impact, threat, and vulnerability; must be captured and entered into MC-CAMS NG.

Marine Corps Mission Assurance – Enterprise Risk Management

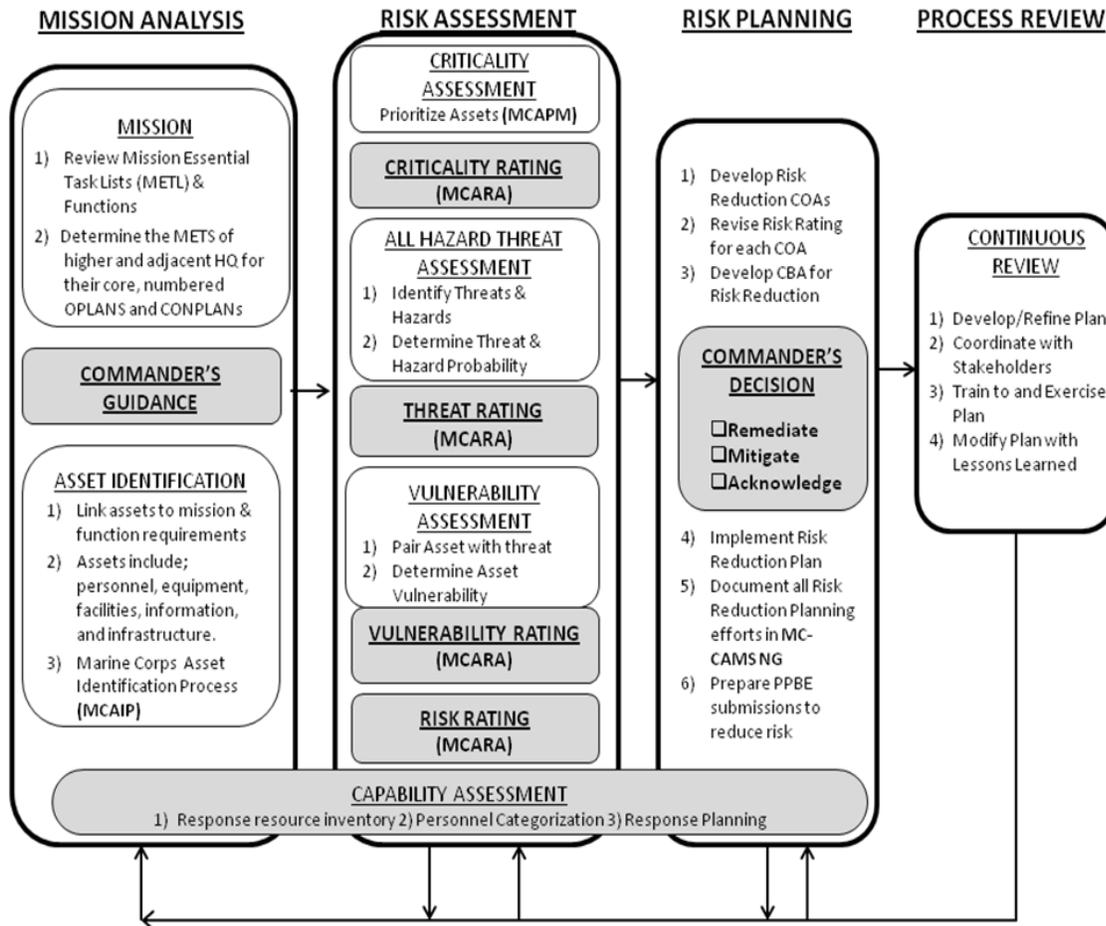


Figure 3 – MCMA-ERM Process

1. Mission Analysis

a. Review command Mission Essential Task Lists (METLs) for any changes and determine the Mission Essential Tasks (METs) of higher and adjacent commands for their core, numbered operational plans, and overseas contingency operations.

b. Commander's Guidance. Obtain the commander's guidance.

c. Asset Identification. There are three major sub-processes involved in identifying critical assets. First, analyze the list of commander-approved METs to identify their Task Critical Assets (TCAs). Second, analyze each TCA to identify its SICAs. Third, analyze each SICA to identify any further SICAs, going at least one node outside of the fence line. During this analysis, BEIs must be collected for each

asset. BEIs provide the necessary information needed to enter into the MC-CAMS NG.

2. Risk Assessment (RA). A RA involves the collection and evaluation of data concerning the criticality of the assets based on mission impacts, likely and probable threats and hazards, degrees of vulnerability, and existing countermeasures to determine the overall risk posture of the asset. Essentially, it is a systematic, rational, and defensible process for identifying, quantifying, and prioritizing risks. Based on the values produced from the criticality, AHTA, and VAs, a RA rating or score is produced. Risk is determined by the following equation: criticality rating x T/H rating x vulnerability rating = risk rating. A risk rating is produced for each specific T/H and vulnerability/asset pairing of data.

a. Criticality Assessment (CA). The CA identifies a command's assets whose degradation or destruction impacts the command's ability to execute its assigned mission or functions, as well as the mission impact or consequence from loss of assets for supported missions. Commanders are required to conduct an annual CA utilizing the following processes and tools to identify missions, functions, and associated assets; determine their criticality score; and determine their impact score.

(1) Mission-Focused Criticality Assessment. Utilizing command-approved METs with their associated conditions, standards, and/or core functions, commanders will identify assets associated with the execution of these METs. Assets can be personnel, equipment, facilities, information and information systems, infrastructure, and supply chains that support the execution of the command's mission and associated critical functions. The analysis will examine those assets whose degradation or destruction impacts the command's ability to execute its assigned mission or function. Department of Defense Instruction (DODI) 3020.45, Vol 1, and Joint Publication (JP) 3-07.2 describe the CAIP in detail. It is the process that must be used to conduct the CA. There are other assets that may not be critical to the execution of the mission or function which may be identified in this criticality process and included in the overall RA process. These non-critical assets could include assets such as high population facilities (e.g., theaters, commissaries, base exchanges, etc.).

(2) Criticality Score. All identified assets will have their criticality score determined by use of the MC-APM. Mission and asset data can be entered into a stand-alone MC-APM

tool, but it must eventually be input into the MC-CAMS NG database. This standardized priority or criticality value is based on all missions supported by the asset. Note: The asset priority value is also the impact value or score that is utilized in the MC-ARA methodology and tool to support the determination of risk of loss to the critical asset.

(2) Updating Critical Asset Risk Profile/Rating.

Critical asset risk profiles/ratings will be updated annually or when changes in the criticality, T/H, or vulnerability occur. Significant increases in risk profiles/ratings may require changes in mitigation/remediation strategies and resource generation priorities.

b. All-Hazard Threat Assessment (AHTA). Execution of the RM process is based on an assessment of the threat and hazard environment in which our forces operate and missions are executed. The development of an AHTA will accomplish two goals: 1) identification of a comprehensive list of threats and hazards, and 2) identification of the likelihood or probability of occurrence of each threat or hazard. The annual AHTA must be tailored to the local environment and ensure all threat information is integrated to meet the collective needs of IEM, CBRNE, AT, CIP, LE, fire and emergency services, PS, and COOP planning. A collaborative effort between the Threat Working Group, CBRNE Working Group, and IEM Working Group will develop the AHTA by fusing information (strategic, operational, and local tactical) derived from liaison between civil and military law enforcement, public safety agencies and departments, as well as meteorological, environmental, public health, and medical syndromic surveillance sources. In the context of assessing risk, the higher the probability or likelihood of a threat or hazard occurring, the higher the risk of loss will be to the asset. Commanders will ensure that the AHTA (HQMC AHTA where applicable) is completed annually. Furthermore, as part of the command RM process, commanders will develop an Integrated and Prioritized Threat Hazard Matrix that reflects the likelihood of assessed threats and hazards (See Figure 3 -).

(1) Threat/Hazard Categories

(a) Threats. Human caused intentional threats include insider threat, cyber, active shooter/lone offender, foreign intelligence, and security services; terrorism to include domestic terrorists, transnational terrorists, and terrorist use of CBRNE; and crime to include non-violent crime,

violent crime, gang activity and narcotics, and conventional/strategic military and civil disturbance.

(b) Hazards. Hazards are broken down into three categories: natural hazards, human-caused-accidental, and technologically caused events. Each of these categories is further described below.

1. Natural hazards. Natural hazards categories include geological, meteorological, and biological. Geological categories include volcano, tsunami, earthquakes, and landslides. Meteorological categories include hurricanes, tornadoes, drought, winter weather, fire, extreme heat, lightning, hail, wind, rain, and flooding. Biological categories include diseases that impact humans or animals such as plague, smallpox, anthrax, West Nile virus, foot and mouth disease, severe acute respiratory syndrome (SARS), pandemic disease, bovine spongiform encephalopathy, etc.

2. Human-caused accidental events. Accidental events can cause disruption to the operation of assets, and the execution of missions supported by those assets. Accidental events can take many forms, such as those that result from individuals making mistakes or causing the accidental event (man-made), to those accidental events that may be caused by technology or technological failures. Examples of various types of accidental events can include, but are not limited to construction accidents (i.e., a back-hoe that unintentionally cuts a power, water, fuel, or communications line), error or mistakes in operating equipment or vehicles, mishaps such as inadvertent chemical spills, and wildlife induced accidental events such as wildlife accessing and damaging assets (i.e. wildlife shorting out electrical transformers).

3. Technologically caused events. Technologically caused events can be the result of aging assets and infrastructure that fail because they are past their normal life cycles, equipment failure caused by power surges or "dirty" power, equipment overheating (such as servers when the Heating, Ventilation, and Cooling (HVAC) system components fail), and software bugs that disrupt systems and networks. Statistics are gathered onsite at specific locations and generally are not available from national databases. Incidence ranges and frequency will have to comply with the Hazard probability definitions (Low, Medium, High, and Critical) to determine overall probability rating.

(2) Threat/Hazard Rating Definitions

(a) Low (.01 to .25). Indicates little or no credible evidence of a threat to the asset or the immediate area where the asset is located.

1. For the identified threat, there is little or no credible evidence of capability or intent and no demonstrated history of occurrence against the asset or similar assets.

2. For the identified hazard, there is little or no credible evidence for potential damage and there is a rare history, or no documented history of occurrence.

(b) Medium (.26 to .50). Indicates a potential threat to the asset or the immediate area where the asset is located. Also indicates there is a significant capability with low or no current intent, which may change under specific conditions and low or no demonstrated history.

1. For the identified threat, there is some evidence of intent, but there is little evidence of a current capability or history of occurrence, but there is some evidence that the threat could obtain the capability through alternate sources. Alternatively, the identified threat evidences a significant capability but there is little evidence of current intent and little or no demonstrated history.

2. For the identified hazard, the hazard has both a moderate potential for damage and a demonstrated history of occurring on an infrequent basis.

(c) High (.51 to .75). Indicates a credible threat against the asset or the immediate area where the asset is located.

1. The identified threat has both the capability and intent, and there is a history that the asset or similar assets are, or have been targeted on an occasional basis.

2. The identified hazard has both a high potential for damage and there is a demonstrated history of the hazard occurring on an occasional basis.

(d) Critical (.76 -1.00). Indicates an imminent threat against the asset or the immediate area where the asset is located.

1. The identified threat has both the capability and intent and there is a history that the asset or similar assets are being targeted on a frequent or recurring basis.

2. The identified hazard has both a significant potential for damage and there is a demonstrated history of the hazard occurring on a frequent basis.

(3) Threat and Hazard Analysis. An analysis must be executed that will identify a baseline of T/Hs that could adversely impact command assets (Figure 3 -). Note that when discussing execution of VAs below, the assessor must align one or more identified T/H to one or more discrete vulnerabilities of assets or the installation that could be exploited by the threat or hazard. The annual AHTA must be integrated into all aspects of the RM process.

Installation / Site Name	T/H Name	T/H Probability Rating Ranges	Probability Rating Source Information	Assessed T/H Probability Rating (Using MC-ARA Tool)	Other Rating Factors - Comments
Camp Zebra	Explosive - 220 lb. Vehicle Borne Improvised Explosive Device (VBIED)		NCIS Threat Assessment dated x/xx/xx; Defense Intelligence Agency (DIA) Threat Assessment dated x/xx; Local installation threat assessment dated x/xx; Past history of similar events occurring, etc.		Site specific intelligence factors; other relevant analysis such as a Design Basis Threat (DBT); identify a specific period for duration of the threat or hazard;

Installation/ Site Name	T/H Name	Assessed T/H Probability Rating (Using CARA Tool)
Camp Zebra	Flooding - Hurricane	
	Explosive - 220 lb. VBIED	HIGH . 60
	Aged Equipment - No Spares	Medium .47
	Electromagnetic Pulse (EMP)	Low . 05

Figure 4 - Integrated and Prioritized Threat/Hazard Matrix

(4) Threat and Hazard Probability Ratings and Definitions. Once a baseline of threats and hazards has been identified, the assessor must analyze those threats and hazards to determine the likelihood or probability of occurrence of each threat and hazard. Probability is defined as the estimate of the likelihood that a threat will cause an impact to the mission or a hazard on the Installation. There are four categories of T/H probability ratings: critical, high, medium, and low. The T/H probability ratings can be found in the MC-ARA stand-alone tool and are also embedded in MC-CAMS NG. The use of these ratings and definitions will facilitate the uniform assessment

of the likelihood or probability of any individual threat or hazard occurring.

c. Vulnerability Assessments. Inspector and Instructor will ensure VAs are conducted annually. A VA is a systematic examination of the characteristics of an installation's system, assets, applications, and its dependencies to identify vulnerabilities that could be susceptible to the effects of any number of threats or hazards. The VA process shall include assessments of food and drinking water. VAs shall also include sea and air ports of embarkation and debarkation, movement routes, and assembly, staging, and reception in support of unit deployments, as appropriate. VAs shall be conducted for off-installation housing, schools, daycare centers, transportation systems, and routes used by DoD personnel and their dependent family members when the Terrorism Threat Level is SIGNIFICANT or higher. VAs will be properly classified per Department of Defense Manual (DODM) 3020.45-M-V3, "Defense Critical Infrastructure Program: Security Classification Manual (SCM)," and the Defense Threat Reduction Agency Security Classification Guide. VAs must be conducted by teams of subject matter experts with backgrounds in different functional areas such as PS, AT, CIP, and Installation Integrated Protection. Inspector and Instructor will prioritize identified vulnerabilities, develop a plan of action to mitigate or eliminate the vulnerabilities, and report the results to the MARFORRES New Orleans (G-3/5 MA) within 90 days of the completed assessment. VAs shall be conducted utilizing the following methods:

(1) Identify and assess all vulnerabilities of the installation or facilities to specifically include all identified critical assets. Vulnerabilities are defined as a weakness or susceptibility of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard effects. Vulnerabilities to a critical asset can result from a wide variety of factors such as: design and construction flaws, environmental factors, proximity to other structures or systems, factors influencing accessibility, personal behaviors of people working in or around the critical assets, or operational practices associated with the critical assets or the installation. Vulnerabilities of a critical asset can also be determined by vulnerabilities to other assets or areas that are not in close proximity to the critical asset. For instance, vulnerabilities in access or perimeter control of an installation may lead to an adversary

gaining access to the Installation, and ultimately to the critical asset located somewhere inside the installation.

(2) Identify degrees of vulnerability. When assessing and identifying vulnerabilities, the assessor needs to make a judgment based on the significance or degree of an identified vulnerability. For example, lack of standoff around a high population building may be identified as a vulnerability, based on Unified Facility Criteria (UFC) requiring 80 feet of standoff. The actual standoff is 79 feet. The significance or degree of vulnerability would be relatively low, as would the impact of exploiting that vulnerability from a threat such as a 220 lb. Vehicle Borne Improvised Explosive Device (VBIED) that the UFC requirement was designed to address. Identifying degrees of vulnerabilities assists in providing a weight associated to each vulnerability, which in turn supports providing an overall RA rating. Vulnerability rating definitions are identified below and can also be found in the MC-ARA tool and MC-CAMS NG.

(3) Vulnerability Ratings Definitions

(a) Low (.01 to .25). Indicates multiple effective layers of integrated countermeasures in place and no known weaknesses through which adversaries, natural hazards, or accidental disruptions would be capable of causing loss of or disruption to an asset.

(b) Medium (.26 to .50). Indicates multiple effective countermeasures in place; however, at least one known weakness exists through which adversaries, natural hazards, or accidental disruption would be capable of causing loss of or disruption to an asset.

(c) High (.51 to .75). Indicates some effective countermeasures in place, but still multiple known weaknesses through which adversaries, natural hazards, or accidental disruptions would be capable of causing loss of or disruption to an asset.

(d) Critical (.76 to 1.00). Indicates minimal effective physical, design, technical, procedural, or behavioral countermeasures in place and many known weaknesses through which adversaries, natural hazards, or accidental disruptions would be capable of causing loss of or disruption to critical assets.

d. Capability Assessment. Commanders shall provide guidance on how subordinates will develop a command, or unit-level evaluation (assessment) to consider the range of identified and projected response capabilities necessary for responding to any type of hazard/threat identified in their AHTA to include the capability to respond to the most likely CBRNE incident. Guidance shall require the installation to conduct a Capability Assessment. The assessment should be conducted on emergency response capabilities to include: Fire and/or Hazardous Materials (HAZMAT) and rescue, LE and/or Security personnel, emergency medical management, and Explosive Ordnance Disposal (EOD) and/or civilian bomb technicians at a minimum. The assessment should also detail those resources that provide immediate response and add the recovery capability to include incident support resources - heavy equipment, sheltering capability, food and messing resources, etc. The capability assessment will include a list of installation/facility resources by type to include external capabilities provided by local community and/or host nation addressed through Memorandums of Understanding (MOUs), Memorandums of Agreement (MOA), and Mutual Aid Agreements (MAAs). Installation/Facility assessments will include a review of personnel, equipment, resources, capabilities, training and exercises, in coordination with State, local, tribal governments, or host nations to promote asset visibility and enhance overall Installation/Facility readiness to include the capability of personnel to operate identified critical assets in a contaminated environment.

(1) Align specific threats and hazards to asset vulnerabilities. Threat-asset vulnerability pairing is conducted to link likely threats and hazards to specific asset vulnerabilities that may be susceptible to a specific threat or hazard. This process is crucial because individual assets may have a greater degree of vulnerability to different threats or hazards. Pairing a threat or hazard with an asset vulnerability will allow for greater precision and understanding of which assets are susceptible to certain threats. This in turn will support the preparation of effective remediation or mitigation plans designed to lower overall risk by incorporating and addressing both T/H and vulnerability analysis in those plans.

3. Risk Planning. While the risk assessment process seeks to evaluate and identify risk of loss to assets based on an asset's criticality (mission impact), the probability of threats and hazards occurring, and associated degrees of vulnerabilities, risk planning is the process of determining options and actions to reduce the risk of loss to the asset, and thus reduce impact

on mission execution. The options/action steps include mitigating the effects the threat will have on the asset, mitigating the effects of loss once T/H event occurs, reconstituting the asset's capabilities after loss or disruption, acknowledging the risk, or simply transferring the risk decision to a higher echelon of command. To complete risk planning, commands can use selected members from the MAWG, or establish a remediation/mitigation team consisting of experienced personnel with necessary expertise for developing risk reduction plans.

a. Risk Decision Packages. Risk decision packages should be developed to assist commanders in risk decisions. Risk decision packages should contain the following elements and are required to be included:

- (1) Executive Summary
- (2) Mission Details
- (3) Threat/Hazard Details
- (4) Asset/Vulnerability Details
- (5) Initial Risk Rating
- (6) Proposed asset Remediation or Mitigation Plan with the Adjusted Risk Rating
- (7) Cost Benefit to Risk Reduction Analysis

The following discusses each risk planning option/action in further detail.

b. Remediation. Remediation is defined as actions taken to correct known deficiencies and weaknesses once a vulnerability has been identified. Remediation involves identifying countermeasures that can be implemented before undesirable events or attacks occur that could exploit the identified vulnerabilities. Planners will prioritize their remediation efforts on those assets with highest impact to supported missions if those assets were lost. Planners will also address the T/H which have the highest rated probability of occurrence, and finally address the most significant asset vulnerabilities which could be exploited by the most likely T/H. To ensure a comprehensive approach is taken, the following subject areas should also be considered:

(1) Pre-event focus of remediation planning:

(a) Step 1 - Doctrine: policy, procedures, guidance, and agreements with internal and external tenant commands/agencies.

(b) Step 2 - Organization: structure and location.

(c) Step 3 - Training: formal, informal, situational.

(d) Step 4 - Material: physical, cyber, financial resources, redundancy.

(e) Step 5 - Leadership: education, knowledge, and experience.

(f) Step 6 - Facilities: physical, access, security, resiliency.

(2) Basic steps to building an effective remediation plan are as follows:

(a) Confirm Stakeholders, Prioritize Risk, and Identify Options. It is important to identify asset owners, mission owners, and other stakeholders that have vested interest in remediating risk to mission assets. MC-APM and/or MC-CAMS NG will be used to prioritize risk to critical assets, as well as to prioritize impact of critical assets on all the missions supported by the asset. These systems generate priority values based on impact to mission and probability of occurrence. Remediation efforts will focus on obtaining optimal risk reduction and the most effective/efficient use of resources.

(b) Analyze Options and Determine the Best Approach. This step focuses on option analysis that determines the option with the most "bang for the buck" should a potential threat or hazard occur, and use of the MC-ARA tool or MC-CAMS NG will assist commanders in analyzing options and determining the best remediation action(s). Executive level planning groups will perform a cost-benefit analysis to balance risk to the asset and/or mission with the resource requirements necessary to execute the remediation action. An example of a Risk Remediation Analysis Matrix is presented in Table 1. This is an example of the Risk Decision package printout available in MC-CAMS NG. In analyzing options to balance risk cost with mission benefits, the following minimum elements must be considered:

1. Step 1 - Identify asset(s) covered by remediation plan.
2. Step 2 - Identify highest asset risk rating (which accounts for criticality, most likely T/H, and most significant vulnerability).
3. Step 3 - Identify cost of risk remediation COAs.
4. Step 4 - Identify revised risk rating should remediation COA be implemented
5. Step 5 - Document COA selection.

Table 1 - Risk Remediation Analysis Matrix

Critical Asset	Threat Rating	Vul. Rating	Risk Rating	Priority	Proposed Remediation Measures	Revised Vul. Rating	Revised Risk Rating
Asset A	Medium	High	Medium	3	Establish an alternate path for access to the Defense Information Systems Network (DISN) and/or the Global Information Grid (GIG).	Low	Low
Asset B	Medium	High	High	1	Use Closed-Circuit Television (CCTV) to search tops of vehicles prior to entry; screen search procedures from other drivers; Harden commercial vehicle gate by installing removable bollards; Ensure Multiple Wavelength Detector (MWDs) are used more frequently as a Random AT Measure (RAM).	Low	Low
Asset C	Medium	Critical	Medium	2	Consider establishing an alternate feed from power supply G. Procure & install Backup (B/U) power generation at Asset E. Increase staffing at Entry Control Points (ECPs) and purchase explosive detection tech to ensure security force has the appropriate tools and manpower to effectively detect explosives.	Medium	Low

(c) Develop and Coordinate the Remediation Plan.

This step requires a Plan of Actions and Milestones (POA&M) that outlines what needs to be done, how it is to be done, who is involved, and when remediation will be completed. The plan must include details concerning the asset, what T/H it is vulnerable to and information concerning the decision to remediate the asset, actions to be taken, resource requirements, and impact to stakeholders.

(d) Implement the Remediation Plan. Once the plan is approved, milestones developed in the above POA&M will be tracked to measure success. Remediation plan effectiveness can be assessed during the command's annual exercise or by HHQ risk assessments, such as MCMAA.

(e) Execute Follow-Up Actions. These actions may include annual self-assessments or other follow-up risk assessment to consider new missions and threats associated with command assets.

(f) Documentation. All remediation plans will be documented in MC-CAMS NG for information sharing purposes.

c. Mitigation. Mitigation is defined as actions taken in response to pre-identified threat, warning, or after an incident occurs which are intended to lessen the potentially adverse effects on a given operation or infrastructure. Again, mitigation planning can be done by selected members of the MAWG or by the establishment of a command remediation/mitigation planning team. As part of RM, commands should evaluate mitigation strategies to reduce risk and support command risk response objectives. The following discusses the mitigation planning process or steps and the types of mitigation plans:

(1) Mitigation Planning Process/Steps:

(a) Step 1 - Develop mitigation goals and objectives. These goals and objectives must be mission-focused, considering the command's METs to include identified conditions and standards for execution. Mission focus helps in the prioritization of time and resources in Step 2.

(b) Step 2 - Identify and prioritize mitigation actions. This step involves identifying potential COA(s) that will reduce risks while supporting optimum cost-benefit strategies. All stakeholders need to be consulted during this step to ensure consideration of all equities and impacts. This step captures the responsible organization for executing the mitigation, the funding source, and timeframe for completion.

(c) Step 3 - Prepare and document an implementation strategy. An implementation strategy is required because there may be many complex variables associated with developing, funding, procuring, training appropriate personnel, and coordinating mitigation measures with other existing security measures. Often, implementation requires a phasing approach

that cuts across numerous commands, agencies, and stakeholders, creating a need for synchronization of priorities. It is recommended that the mitigation implementation strategy be exercised to ensure desired results are achieved and any negative cascading affects are identified and addressed.

(d) Step 4 - Implement the plan and monitor progress. Commands will document their mitigation plans in MC-CAMS NG as required by DOD policy. Also, commands will take every opportunity to measure the effectiveness of their mitigation plans through annual exercises and scheduled risk assessments.

(2) Types of mitigation plans/planning required. When mitigating risks to command mission assets and supporting infrastructure, the planning process must include the development of the following plans:

(a) Installation Emergency Response Priorities. This plan establishes first responder emergency response priorities with a focus on mission continuity.

(b) Utility Restoration Priorities. This plan identifies the priority of work for restoring utility infrastructure (i.e., electricity and water) which specifically supports critical asset operations. Priority restoration plans shall be identified for critical assets (Tiers I-III), including those critical assets owned by tenant commands within the overall host installation priority planning.

(c) Installation Security Response Priorities/Plans. These plans address actions taken in concert with T/H indications and warnings which necessitate an escalation in security response. Examples of these plans include the Security Force Augmentation Plan, Random AT Measures Implementation plan, FP Condition Action Sets Plan. Security response and protection measures priorities should be identified for location housing critical assets, including those critical assets owned by tenant commands within the overall host installation security response priority planning.

(d) COOP Plans. Leverage and integrate Marine Corps COOP requirements with existing MA policies and programs focused on the protection of critical resources and infrastructure and continuation of mission essential functions. See reference (c).

(e) Reconstitution Plans. Reconstitution is the process by which surviving and/or replacement organization personnel resume normal operations from the original or replacement primary operating facility. Organizations are encouraged to tailor their Reconstitution Plan Annex to meet their specific continuity planning and operational needs.

(3) Documentation. All mitigation plans will be documented in MC-CAMS NG for information sharing purposes.

d. Acknowledgement of Risk. After review of the risk assessment data, if commanders deem the overall risk to mission critical assets and high value assets to be acceptable, the commander can elect to forego remediation and mitigation planning and the implementation of security countermeasures. It is the commander's prerogative to acknowledge risk where appropriate in the commander's judgment and based on being fully informed of all RA data. Historically, reasons for accepting risk revolve around cost-benefit analysis results, lack of resources to implement a desired risk reduction measure, or lack of a significant threat or hazard.

e. HHQ Risk-Informed Decision Making. When risk cannot be reduced to a minimum acceptable level after executing remediation and mitigation measures, the deferral of risk-based decision making to the next higher echelon of command is required to leverage additional resources.

f. Documentation. All risk decisions to include remediation, mitigation, acknowledgement, and transfer must be documented in MC-CAMS NG for information sharing purposes.

g. Planning, Programming, Budgeting, and Execution (PPBE) System. The PPBE is the business process of allocating resources within the DoD. The PPBE is a cyclic process that provides the mechanisms for decision-making and the opportunity to reexamine previous decisions in light of changes in the environment (i.e., evolving threat, changing economic conditions). The ultimate objective of the PPBE is to provide COCOMs with capabilities that include the best mix of forces, equipment, and support attainable within established fiscal constraints to accomplish their mission. It is important for program managers and their staff to be aware of the milestones for the financial managers during the PPBE process to ensure critical information is provided at the appropriate time to the appropriate agencies for both programming future funding and executing the budget. Failure to provide punctual information

during the PPBE process will result in the loss of potential funding. Planning and programming resources is done through the POM process and budgeting, and execution is done in the execution of the Five-Year Development Plan (FYDP).

(1) Program Objective Memorandum Process (POM). The POM process is the primary method of programming resources. The POM process does not address the current year funding; rather, it addresses the programming of funding execution one year in advance of the current FYDP. POM submissions are evaluated by different Program Evaluation Boards (PEBs) for each type of appropriation.

(a) The Installation PEB evaluates POM nominations for the Installation Marine Corps Program Codes (MCPC) (such as MCPC 630104 Security). POM nominations are submitted by the Marine Corps Forces (MARFOR) level G8 and or the appropriate HQMC Program Manager.

(b) Construction requirements associated with installation perimeter security requirements are submitted by the G4 Facilities Engineers either as a Facilities, Sustainment, Restoration and Modernization, or Military Construction (MILCON) requests.

(c) Procurement funding is done exclusively by Marine Corps Systems Command (MARCORSYSCOM), but submitted by Program Managers in Marine Corps Combatant Development Command (MCCDC) or by Plans, Policies, and Operations Security Division for Marine Corps Electronic Security System requests. Resource requirements for electronic security system are submitted through the Electronic Security System portal, and the Security Division prepares POM initiatives based on those needs. The other way to implement POM for material solutions for new capabilities is the Universal Need Statement (UNS) submitted to MCCDC.

4. Process Review. Once the RM process is complete, it is essential that a thorough review of the overall process be conducted. This is typically done during the annual program review. This section discusses the components of the RM review process.

a. Refine Plan. Necessary revisions to the MA plan can be documented and initiated during this portion of the process. As noted, the RM process must be executed as a cycle. By using

this framework, revisions can always be pursued and the MA program can be continually improved.

b. Coordinate with Stakeholders. Commanders should ensure that stakeholders in the military and local civilian communities are involved in the process review. This collaboration will ensure that supporting plans align with the RM process. Stakeholders from the local community can also identify strengths and weaknesses, focusing on collaboration between the military and civilian agencies. Complex operating environments magnify the importance of coordinating with expeditionary forces. In order for expeditionary commander's to effectively manage risk, his or her ATO and MA professionals should possess a solid understanding of the local customs, culture, and society in which they operate. Interfacing and coordinating preventive and/or response measures with local stakeholders may ensure a more robust security posture. Coordinating with local stakeholders should never be done at the risk of endangering DOD personnel, assets, or USMC missions.

c. Exercise and Modify Plan. The final stage in the RM process review is to exercise the plan and make adjustments as needed. Once the all-hazards RM plan is implemented, gaps may be identified; if this occurs, commanders will ensure that the plan is modified to address these issues.

Acronyms and Definitions

Part I: Acronyms

4S	Sense, Shape, Shield, and Sustain
ACL	Advocate Capabilities List
AGL	Advocate Gap List
AHS	Alternate Headquarters Site
AHTA	All Hazards Threat Assessment
AOR	Area of Responsibility
AT	Antiterrorism
ATO	Antiterrorism Officer
B/U	Backup
BEI	Baseline Elements of Information
C2S	Command and Control System
CA	Criticality Assessment
CAIP	Critical Asset Identification Process
CBRN	Chemical, Biological, Radiological, and Nuclear
CBRNE	Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive
CCTV	Closed-Circuit Television
CDRUSNORTHCOM	Commander, United States Northern Command
CI	Counterintelligence
CIP	Critical Infrastructure Program
COA	Course of Action
COC	Combat Operations Center
COCOM	Combatant Command
COMMARFORNORTH	Commander, Marine Forces North
COMMARFORRES	Commander, Marine Forces Reserve
CONOPS	Concept of Operations
CONUS	Continental United States
COOP	Continuity of Operations
COP	Common Operating Picture
CPO	CBRNE Protection Officer
CT	Counterterrorism
DBT	Design Basis Threat
DC PP&O	Deputy Commandant Plans, Policies, and Operations
DCA	Defense Critical Asset
DCIP	Defense Critical Infrastructure Program
DIA	Defense Intelligence Agency
DISN	Defense Information Systems Network
DOD	Department of Defense
DODI	Department of Defense Instruction
DODM	Department of Defense Manual

DRRS-MC	Defense Readiness Reporting System - Marine Corps
DTRA	Defense Threat Reduction Agency
DW	Destructive Weather
ECP	Entry Control Point
EFD	Expeditionary Force Development System
EM	Emergency Management
EMP	Electromagnetic Pulse
EOD	Explosive Ordnance Disposal
ESS	Electronic Security System
ESSIDS	Electronic Security System/Intrusion Detection System
F&ES	Fire and Emergency Services
FACMAPS	Functional Area Checklist Management and Processing
FHG	Force Headquarters Group
FIE	Foreign Intelligence Entities
FP	Force Protection
FPCON	Force Protection Condition
FPR	Force Protection Readiness
FSRM	Facilities, Sustainment, Restoration, and Modernization
FY	Fiscal year
FYDP	Five-Year Development Plan
GIG	Global Information Grid
HAZMAT	Hazardous Materials
HHQ RA	Higher Headquarters Risk Assessments
HQMC	Headquarters Marine Corps
HVAC	Heating, Ventilation, and Cooling
IA	Information Assurance
IATP	Individual Antiterrorism Plan
ICS	Incident Command System
IEM	Installation Emergency Management
IG	Inspector General
IGMC	Inspector General Marine Corps
ISOPREP	Isolated Personnel Report
IT	Information Technology
JP	Joint Publication
JSIVA	Joint Staff Integrated Vulnerability Assessment
LE	Law Enforcement
MA OAG	Mission Assurance Operational Advisory Group
MA	Mission Assurance
MAA	Mutual Aid Agreement
MAAT	Mission Assurance Assessment Team
MAEC	Mission Assurance Executive Council

MAGTF	Marine Corps Air-Ground Task Force
MAPEC	Mission Assurance Program Executive Committee
MARADMIN	Marine Administrative Message
MARCORSPTFAC	Marine Corps Support Facility
MARCORSYSCOM	Marine Corps Systems Command
MARDIV	Marine Division
MARFOR	Marine Corps Forces
MARFORCOM	Marine Forces Command
MARFORNORTH	Marine Forces North
MARFORPAC	Marine Forces Pacific
MARFORRES	Marine Forces Reserve
MAW	Marine Aircraft Wing
MAWG	Mission Assurance Working Group
MC-AIP	Marine Corps Asset Identification Process
MC-APM	Marine Corps Asset Prioritization Methodology
MC-ARA	Marine Corps Asset Risk Assessment
MC-CAMS NG	Marine Corps Critical Asset Management System Next Generation
MCCDC	Marine Corps Combatant Development Command
MCCIP	Marine Corps Critical Infrastructure Protection
MCFDS	Marine Corps Force Development System
MCICOM	Marine Corps Installations Command
MCLL	Marine Corps Center for Lessons Learned
MCMAA	Marine Corps Mission Assurance Assessment
MCMA-E	Marine Corps Mission Assurance Enterprise
MCMA-ERM	Marine Corps Mission Assurance-Enterprise Risk Management
MCO	Marine Corps Order
MCOC	Marine Corps Operations Center
MCPC	Marine Corps Program Code
MCRC	Marine Corps Reserve Center
MCSCP	Marine Corps Service Campaign Plan
MCSPFACNOLA	Marine Corps Support Facility New Orleans
MCTL	Marine Corps Task List
MEF	Mission Essential Functions
MET	Mission Essential Task
METL	Mission Essential Task List
MILCON	Military Construction
MLG	Marine Logistics Group
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MOU/A	Memoranda of Understanding/Agreement
MP	Military Police
MROC	Marine Requirements Oversight Council

MSC	Major Subordinate Command
MWD	Multiple Wavelength Detector
NCIS	Naval Criminal Investigative Service
NIMS	National Incident Management System
NMS	National Military Strategy
NOLA	New Orleans
OCONUS	Outside Continental United States
OPFOR	Operating Forces
OPR	Office of Primary Responsibility
OPREP	Operations Report
OPSEC	Operations Security
OSD	Office of the Secretary of Defense
PA	Protection Advocate
PEB	Program Evaluation Board
PEBs	Program Evaluation Boards
P-ESG	Protection Executive Steering Group
POA&M	Plan of Actions and Milestones
POM	Program Objective Memorandum
PP&O	Plans, Policies, and Operations
PPBE	Planning, Programming, Budgeting, and Execution
PR	Program Review
PRMS	Personnel Recovery Mission Software
PS	Physical Security
RA	Risk Assessment
RAM	Random Antiterrorism Measure
RDPs	Risk Decision Packages
RFI	Request for Information
RM	Risk Management
SAF	Standalone Facility
SCM	Security Classification Manual
SE	Supporting Establishment
SECDEF	Secretary of Defense
SICA	Supporting Infrastructure Critical Asset
SIPRNET	Secure Internet Protocol Router Network
SIR	Serious Incident Report
SOP	Standard Operating Procedure
T/O/T/E	Table of Organization/Table of Equipment
TACON	Tactical Control
TAD	Temporary Additional Duty
TCA	Task Critical Asset
TDY	Temporary Duty
TIC	Toxic Industrial Chemical
TIM	Toxic Industrial Material
TT	Travel Tracker
TWG	Threat Working Group
UFC	Unified Facility Criteria

UFR	Unfunded Requirement
UJNS	Urgent Universal Needs Statement
UNS	Universal Need Statement
USMC	United States Marine Corps
USNORTHCOM	United States Northern Command
USPACOM	United States Pacific Command
VA	Vulnerability Assessment
VBIED	Vehicle Borne Improvised Explosive Device

Part II: Definitions

Advocate Capabilities List (ACL). Marine Corps capabilities comprised of functional tasks, applicable conditions, and required standards.

Advocate Gap List (AGL). An assessment of the ability of the programmed force to provide the capabilities called for in the ACL.

All-Hazards and Threats. Any incident, natural or manmade, including those defined in DoDI 6055.07 that warrants action to protect the life, property, health, and safety of military members, dependents, and civilians at risk; and minimize any disruptions of installation operations. Also referred to as All-Threats/All-Hazards. (DoDI 6055.17)

Antiterrorism (AT). Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces. Also called AT. (JP 1-02)

Asset. A distinguishable entity that provides a service or capability. Assets are people, physical entities, or information located either within or outside the United States and employed, owned, or operated by domestic, foreign, public, or private sector organizations. (DoDD 3020.40)

Chemical, Biological, Radiological, Nuclear and High-Yield Explosive (CBRNE). An emergency resulting from the deliberate or unintentional release of nuclear, biological, radiological, or toxic or poisonous chemical materials, or the detonation of a high-yield explosive. (JP 1-02)

Common Operating Picture (COP). A single identical display of relevant information shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness. Also called COP. (JP 3-0)

Continuity of Operations (COOP). An organization's ability to continue its MEFs with little or no interruption during, and in the aftermath of an emergency. (MCO 3030.1)

Counterterrorism (CT). Operations that include the offensive measures taken to prevent, deter, preempt, and respond to terrorism. Also called CT. (JP 1-02)

Critical Asset Identification Process (CAIP). Provides a standardized methodology for identifying assets that are critical to the execution of a command's missions, functions, and/or core capabilities. Used to conduct the criticality assessment portion of the Marine Corps Risk Assessment process across all mission areas and programs. (JP 3-07.2 / DoDM 3020.45 (Vol. 1)

Defense Critical Asset (DCA). An asset of such extraordinary importance to operations in peace, crisis, and war that its incapacitation or destruction would have a serious, debilitating effect on the ability of the DOD to fulfill its missions. (DODD 3020

Defense Critical Infrastructure Program (DCIP). Program that takes action to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Depending on the risk, these actions could include changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding; etc. Also called CIP. (DODD 3020.40)

Force Protection (FP). Actions taken to prevent or mitigate hostile actions against DoD personnel (to include family members), resources, facilities, and critical information. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease. Also called FP. (JP 1-02)

Installation Emergency Management (IEM). A program designed to provide the integrated planning, execution, and management of response efforts (designed or intended) to prepare for, respond to, and recover from the effects of an "all-hazard" incident, to include but not limited to, natural hazards, human-caused events, and technologically caused events to protect the force and allow freedom of maneuver to meet National Military Strategic requirements. (MCO 3440.9)

Marine Corps Air-Ground Task Force (MAGTF). A term used by the Marine Corps to describe the principal organization for all missions across the range of military operations. MAGTFs are a balanced air-ground, combined arms task organization of Marine Corps forces under a single commander that is structured to accomplish a specific mission.

Marine Corps Force Development System (MCFDS). A process used to develop future warfighting capabilities to meet national

security objectives. The system guides the identification, development, and integration of warfighting and associated support and infrastructure capabilities for the MAGTF. Also called MCFDS. (MCO 3900.15A)

Marine Requirements Oversight Council (MROC). Principal body advising the Commandant on policy matters related to concepts, force structure, and requirements validation. Also called MROC. Marine Corps Critical Asset Management System Next Generation (MC-CAMS NG). The official data management system that supports MA life cycle activities for the Marine Corps. This system captures data focused on tying core Marine Corps operational and Title 10 capabilities, functions, and missions to the assets and infrastructure "critical" to the execution of those capabilities, functions, and missions.

Marine Corps Mission Assurance Enterprise Roadmap (MCMA-ER). Provides the framework and Service-level direction to develop and integrate protection-related programs, activities, functions, and operational capabilities using a comprehensive, all-hazards approach. Specifically, this approach is structured to enhance the overall protection of the OPFOR and Supporting Establishment (SE) in order to ensure mission execution and accomplish the specified and implied tasks identified in the Marine Corps Service Campaign Plan (MCSCP). The MCMA-E aligns planning and resource activities; synchronizes policy, doctrine, and capabilities development; and integrates functional area management across the enterprise.

Mission Assurance (MA). Both an integrative framework and a process to protect or ensure the continued function and resilience of capabilities and assets - including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains - critical to the performance of DoD MEFs in any operating environment or condition. (DoD Mission Assurance Strategy, May 2012)

Mission Assurance Assessment Team (MAAT). A group of subject matter experts established by the HQMC PP&O Physical Security Division to conduct an all-threats/all-hazards risk assessment to provide base and installation commanders with a clear understanding of risk exposure. These assessments integrate all aspects of MA, providing the commander with information necessary to support an integrated risk management decision process. (CMC MSG DTG: 141427Z Apr 10)

Mission Assurance Operational Advisory Group (MA OAG). A forum chartered to make recommendations on how the USMC should organize, man, train, and equip USMC OPFOR and the SE to protect and sustain MEFs, personnel, and resources. The MA OAG recommends protection program priorities and provides direct interaction among the Deputy Commandants, other Headquarters Marine Corps Departments, and the SE, as well as other representatives concerned with issues involving protection programs.

Mission Assurance Executive Council (MAEC). An installation- or command-level executive body that assesses, integrates, and synchronizes protection-focused capabilities, programs, and resource investments - including existing, planned and emergent requirements for identifying risks, and informing and prioritizing protection COAs to the commander for decision so that finite resources can be better allocated. The MAEC provides a single, multi-disciplinary entity to review all-threats/all-hazards protection and MA issues, recommend changes, recommend resource priorities, and monitor the implementation of MA policy.

Mission Assurance Working Group (MAWG). A body comprised of a diverse mix of asset owners, mission owners, program managers, and non-DoD support or civilian community-focused entities at the command and installation level. The MAWG facilitates the interdisciplinary coordination between subject matter experts designed to assist with the MA advocacy process.

National Military Strategy (NMS). A document approved by the Chairman of the Joint Chiefs of Staff for distributing and applying military power to attain National Security Strategy and National Defense Strategy objectives. Also called NMS. (JP 3-0)

Physical Security (PS). Active and passive measures designed to prevent unauthorized access to personnel, equipment, installations, material and documents, and to safeguard them against sabotage, damage, and theft. Also called PS.

Planning, Programming, Budgeting, Execution (PPBE). Process used to allocate resources within the Department of Defense. The PPBE is a cyclic process that provides the mechanisms for decision making and provides the opportunity to reexamine prior decisions in light of changes in the environment.

Program Evaluation Board (PEB). Establishes the funding priorities for the next POM submission. The five PEBs consist

of: Warfighting, Training, Manning, Operating Forces and HQ, and Support.

Program Objective Memorandum (POM). An annual memorandum in prescribed format submitted to the Secretary of Defense (SECDEF) by the DoD Component heads, which recommends the total resource requirements and programs within the parameters of SECDEF's fiscal guidance. The POM is a major document in the PPBE process, and the basis for the component budget estimates.

Protection. Preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area. (JP 1-02).

Protection Executive Steering Group (P-ESG). Provides senior-level strategic guidance and oversight for the MA OAG, and serves as the Protection Advocate's senior forum for strategic interaction with various POM/MCFDS enterprise bodies and processes. The P-ESG also reviews/approves MA OAG recommendations; provides guidance on issues forwarded by the MA OAG; and, in turn, endorses, settles, or provides recommendations for issue resolution to the Protection Advocate. The P-ESG also ensures that protection-related issues and requirements are fully coordinated with other advocates and POM/EFDS enterprise bodies, as appropriate.

Risk. Probability and severity of loss linked to threats or hazards. (JP 3-07.2)

Risk Management (RM). A continual process or cycle where risks are identified, measured, and evaluated; countermeasures are then designed, implemented, and monitored to see how they perform, with a continual feedback loop for decision-maker input to improve countermeasures and consider tradeoffs between risk acceptance and risk avoidance. (DODI 6055.17)

Standalone Facility (SAF). A facility that resides off a DOD installation. SAFs are embedded in communities. While some have barriers that define an operational area, most are an integral part of their environment where they reside and have no organic security or emergency response capabilities. Most SAFs are dependent upon external community or military agencies for security and intelligence analysis. Each requires careful consideration of protective measures and application of resources specifically tailored to the existing threat.

Supporting Establishment (SE). Includes HQMC, MCRC, and other non-MAGTF organizational elements who primarily serve in the capacity as advocate or proponent for training, manpower, headquarters, acquisition, logistics, and installations. (MARADMIN 422-07, MARADMIN 597-12)

Supporting Infrastructure Critical Asset (SICA). An asset that supports the functioning or operation of a TCA such that the asset's loss, degradation, or denial will result in the inability of the TCA to function or operate as intended in the execution of its associated task/MET or function. In other words, a TCA cannot operate or function without an SICA being available and functioning.

Task Critical Asset (TCA). An asset of such extraordinary importance that its incapacitation or destruction would have a serious and debilitating effect on the ability to execute the MET, MEF, or capability it supports. A TCA is an asset that is utilized to directly execute an essential business function or operational task/mission (e.g., a satellite used for a surveillance task).