**DEPARTMENT OF THE NAVY**
CHIEF OF NAVAL AIR TRAINING
250 LEXINGTON BLVD SUITE 102
CORPUS CHRISTI TX 78419-5041

CNATRAINST 3058.2
00D/00J
1 AUG 18

CNATRA INSTRUCTION 3058.2

From: Chief of Naval Air Training

Subj: RISK MANAGEMENT PROGRAM

Refs: (a) DODD 3020.40 – Defense Critical Infrastructure Protection (DCIP)
(b) DODINST 8510.01 – Risk Management Framework (RMF)
(c) OPNAVINST 3500.39C – Operational Risk Management (ORM)
(d) FCC/C10F INST 5210.1A – Manager's Internal Control (MIC) Program
(e) FCC/C10F Strategic Plan (2015-2020)
(f) EKMS-1B
(g) NIST SP800-30 – Guide for Conducting Risk Assessments

1. Purpose. This program will collate all Department of Defense (DoD) and Department of the Navy (DoN) policies, programs, and requirements (Refs a through g) to address organizational and technical risks for Chief of Naval Air Training, into one local program with mutually supportive and aligned instructions. This program is meant to support decision-making and provide actionable plans in an effort to minimize the impact to any realized events. Figure (1) provides a visual representation of a tiered approach and how the various programs and documents fit within this over-arching risk management program. The program will:

a. Identify threats and vulnerabilities with probability of occurrence and impact to calculate risk associated with the organization (Tier 1), mission and processes (Tier 2), and assets (Tier 3) in accordance with ref (g).

b. Determine the lines of business (aka functions) that are critical to our mission and that of our customers.

c. Provide a plan for immediate triage from any catastrophic incident.

d. Provide a plan for restoring critical lines of business.

e. Provide individual information system contingency plans (ISCP) to restore services as rapidly as possible.

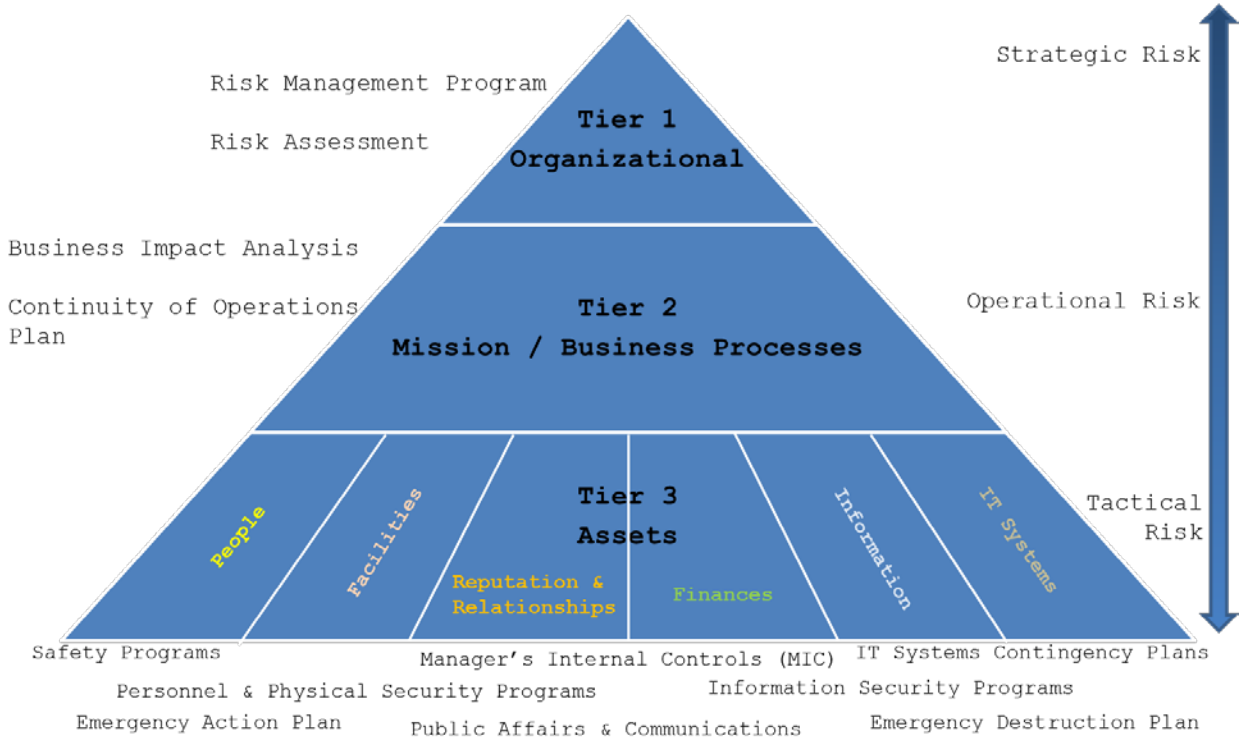


Fig. 1 – Tiered Risk Management Program

2. Scope. This program is comprehensive in that it will assess risk to the organization, people, processes, systems, and data – anything that is safety or security related. The following local instructions and documents will comprise the whole of this program, with Figure (2) providing the program hierarchy.

a. Comprehensive Risk Assessment

b. Business Impact Analysis (BIA)

c. CNATRA Safety Program (CNATRAINST 3750.22J)

d. Operations Security (OPSEC) Program (CNATRAINST 5510.1B)

e. Personnel Security Program (CNATRAINST 5510.1B)

f. Anti-Terrorism / Force Protection Security Plan (CNATRAINST 3300.1C)

g. Cybersecurity Policy and Program (CNATRAINST 5239.3B)

h. Emergency Action Plan (EAP) (CNATRAINST 5510.1B)

i. Emergency Destruction Plan (EDP) (CNATRAINST 5510.B)

j. Continuity of Operations Plan (COOP) (CNATRAINST 3030.1A)

k. Information System Contingency Plan (ISCP)– IT

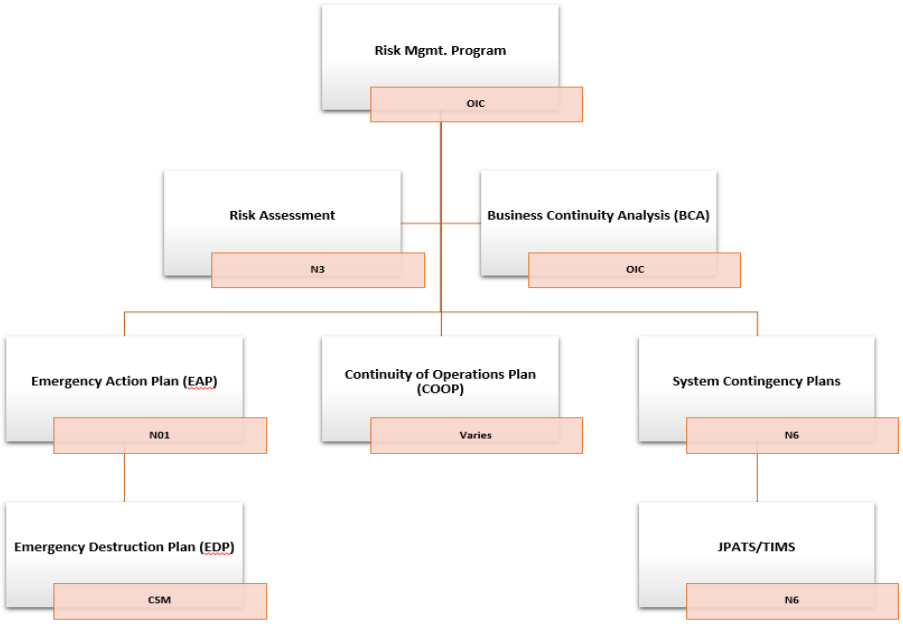


Fig. 2 – Risk Products Hierarchy

3. Policy. It is essential that risk management planning and tasks align to close any gaps and/or resolve any conflicts between the various governing policies, programs, and processes. Local programs must do more than simply meet a "check in the box" for a policy. They must be understood by everyone they affect and most importantly, actionable when needed.

a. Program Establishment. Each of the documents listed in paragraph two will be developed or updated, and implemented within six months of this instruction.

b. Program Management. Each of the subordinate documents of this program shall be reviewed annually for updates that may be required due to changes in risk factors, organizational mission or functions, and/or IT systems.

4. Risk Realization Lifecycle. Each of the products that comprise this program are intended to meet specific areas of a coordinated response process, not as stand-alone plans that are the sole resource for a given event. The basic process is depicted in Fig. (3).

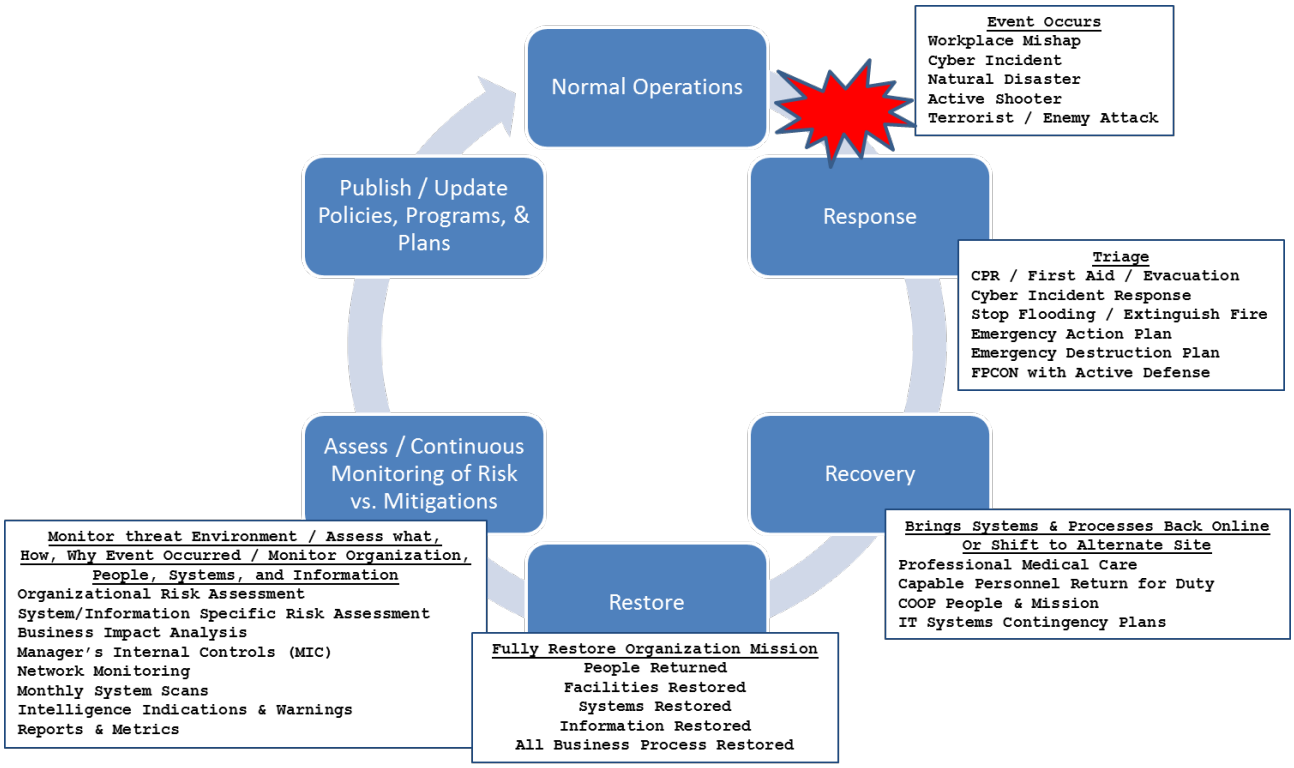


Fig. 3 – Risk Realization Lifecycle

a. Example for severe flooding. The following example is provided to demonstrate how the various products from the Risk Management Program will be used in preparation for, and during a real life event.

(1) The Risk Assessment identifies that the risk of flooding due to significant rain is high, but low from a hurricane or tsunami. Due to the risk calculation that includes probability and impact, it is determined that the risk cannot be accepted or transferred, and must be mitigated through controls and response plans.

(2) The BIA identifies the core mission areas of the command, what their impact would be to the organization, and broadly what the impact would be to customers. This allows leadership to prioritize mitigation and response plan efforts for resources and timing.

(3) Based on input from the Risk Assessment, the EAP provides a succinct process to:

(a) Account for assigned personnel and families.

(b) Protect facilities and respond to critical damage.

(c) Protect systems and respond to critical damage/outages (d). Provide security of personnel, facilities, and national security information.

(4) The EDP, if/when initiated by the Emergency Action Plan, provides a succinct process to securely store, transport, and/or destroy communications security (COMSEC) equipment and keying material, and classified documents and digital data if the flooding cannot be contained and the building is evacuated.

(5) The COOP provides the priorities and processes to transfer and/or restore mission areas based on the BIA. It is supported by actions in the EAP to ensure that personnel and facilities are able to support mission, the results of the EDP if COMSEC and access to required classified information and information systems is available, and the status of individual ISCP for whether the mission-specific IT systems are operational or not. The COOP also sets priorities for resources to support ISCP.

(6) ISCP provides concise response actions to restore the hardware, software, configurations, and data to support mission areas. Actions may support partial or full restoration in Corpus Christi, an alternate temporary location, or by transferring the data to an alternate permanent site.

(7) Once the crisis has passed, and depending on the amount of damage, long-term planning and processes will be initiated as required to return personnel, permanently restore or replace facilities, permanently restore or replace IT systems, and to permanently and fully restore the organizations mission areas and day-to-day operations.

(8) When the organization and mission is fully restored, an assessment of the event and actions taken is conducted to determine the need for new controls and updates to existing plans and processes to prevent the event from reoccurring, or mitigate the risk if it does.

(9) Finally, the command resumes normal operations with continuous monitoring.

5. Roles & Responsibilities.

a. Chief of Naval Air Training. Serves as the Chief Risk Officer and Program Manager, with the authority to make risk-based decisions (when not limited by higher authority) and ultimate responsibility for the commands mission, facilities, systems, and people. Specifically, CNATRA shall:

(1) Establish, maintain, and update this instruction as necessary.

(2) In accordance with ref (g), lead the collective effort for the development of the Risk Assessment, ensuring that all sources (e.g., Defense Threat Reduction Agency assessments, Force Protection Conditions (FPCON), intelligence reports, etc.) are incorporated in documented plans and operational decisions.

b. Chief of Staff (COS). Lead and manage tasking related to the development and implementation of this program and all subordinate products, ensuring that everything is completed within six months and updated as necessary. Specifically, the COS shall:

(1) Generate and manage a Plan of Action and Milestones with general tasks and timeline to develop and implement this program.

(2) Act as the lead for the BIA, to determine critical, essential, and routine lines of business (aka functions and tasks), prioritize identified lines of business, and ensure the planning and resources to mitigate risk and restore capabilities are in place and executed properly when activated.

(3) Participate in the EAP, EDP, and COOP development, and any ISCP that are required for detachment to complete its mission, functions and tasks.

c. Operations Officer (N3 Department Head). Responsible for the detachment's primary mission areas consisting of enterprise network services, technical control facility services, video-teleconferencing services, and support mission area of facilities management, ensuring all are protected and resilient to the greatest extent possible. Specifically, the Operations Officer shall:

(1) Lead the development of the COOP to ensure that critical services are restored as quickly as possible, on-site or at an alternate location, or are transferred to an alternate service provider with the goal to minimize operational impact to our customers.

(2) Develop and conduct annual COOP exercises.

(3) Monitor intelligence to predict potential events/incidents, monitor risk sources to detect occurring events/incidents, and lead the execution of all operational plans (COOP and N6 ISCP) to mitigate impact and restore services as quickly as possible.

(4) Participate and support the BIA, EAP, and EDP development.

d. Administration Officer (N01 Department Head). Responsible for the safety, accurate accounting, and evacuation of personnel. Specifically, the Admin Officer shall:

(1) Lead the development and execution of the EAP to ensure that processes are in place to respond to emergencies, communicate evacuation orders, and account for all personnel and their families.

(2) Develop and conduct semi-annual EAP drills and exercises.

(3) Participate and support the BIA and COOP development, and those ISCP that are required to support command functions and tasks.

e. Command Information Officer (CIO). Responsible for cybersecurity compliance, risk analysis, mitigation planning, and cyber incident response. Specifically, the CIO shall:

(1) Lead the systems authorization (previously known as certification and accreditation) process for all IT systems operating at the detachment. This will establish the initial known and validated cybersecurity baseline with policy and standards compliance.

(2) Maintain the command Cybersecurity Policy and Program instruction, ensuring it is current, relevant, and actionable.

(3) Ensure that cyber threats and IT vulnerabilities are fully incorporated from the organization (Tier 1) to specific lines of business (Tier 2) for the COOP and down to each IT system (Tier 3) for their respective contingency plans.

(4) Participate and support the BIA, EAP, EDP, COOP, and all ISCP development.

(5) Lead incident handling processes for cyber events, ensuring proper and timely reporting, approved mitigating actions are completed with the intent to protect forensic evidence, and scanning for residual or additional malware is accomplished.

(6) Develop and conduct semi-annual incident response drills and exercises.

f. Safety Officer. Responsible for the Command's Safety Program and alignment of supporting safety instructions and programs (e.g., electrical safety and fire protection). Specifically, the Safety Officer shall:

(1) Ensure the Command's instructions are current, relevant, and actionable.

(2) Ensure safety measures are in place to mitigate risk to personnel and assessed/tested at least annually, if not required more frequently per higher governing policies.

g. Physical Security Officer. Responsible for leading the Command to meet all physical security requirements, and assessing and modifying (when required) physical security measures to provide for adequate defense of the organization's personnel, facilities, and information. Specifically, the Physical Security Officer shall:

(1) In coordination with the AT/FP Officer, ensure that the Detachment Physical Security Program and AT/FP Plan instructions are current, relevant, and actionable.

(2) Ensure all required training for active duty and civilians are completed

h. Anti-Terrorism / Force Protection (AT/FP) Officer. Responsible for the risk mitigation plan and actions to protect the Detachment from terrorist attacks. Specifically, the AT/FP Officer shall:

(1) In coordination with the Physical Security Officer, ensure that the Command Physical Security Program and AT/FP Plan instructions are current, relevant, and actionable.

(2) Ensure security measures are in place IAW FPCON requirements, and that personnel are trained and prepared to respond if necessary.

i. Operations Security (OPSEC) Officer. Overall responsible for program management, mitigation plan, and personnel awareness training for the risks associated with OPSEC.

j. Other Department Heads (N4 and N7). Participate and support the BIA, EAP, EDP, and COOP development, and ISCP required to support departmental functions and tasks.

6. Duration. This instruction will remain in effect until cancelled or superseded.

S. B. STARKEY
Chief of Staff