DEPARTMENT OF THE NAVY
COMMANDER
NAVAL EDUCATION AND TRAINING COMMAND
250 DALLAS STREET
PENSACOLA, FLORIDA 32508-5220

NETCINST 5200.6
N00G
11 Dec 2024

NETC INSTRUCTION 5200.6

From: Commander, Naval Education and Training Command

Subj: NETC INTEGRATED RISK MANAGEMENT PROGRAM

Ref: (a) Federal Managers' Financial Integrity Act (FMFIA) of 1982
(b) GAO-14-704G, Standards for Internal Control in the Federal Government of September 2014
(c) OMB Circular A-123, Management Responsibility for Enterprise Risk Management and Internal Control of 15 July 2016
(d) OPNAVINST 5200.25F
(e) SECNAVINST 5200.35G
(f) NETCINST 5040.1D
(g) NETCINST 5000.1D
(h) OPNAVINST 3500.39D

Encl: (1) Definitions

1. Purpose. To provide policies and assign responsibilities for the Naval Education and Training Command (NETC) Integrated Risk Management (IRM) Program. This instruction cancels the Managers' Internal Control Program (MICP).

2. Cancellation. NETCINST 5200.1A.

3. Scope. This instruction is applicable to all NETC Headquarters (HQ) and domain personnel. All commanders, commanding officers (CO), and directors are responsible for establishing and monitoring internal controls (or management safeguards) for their commands. References (a) through (h) apply. Internal controls are built into work processes by managers and process owners to provide reasonable assurance that resources are safeguarded; information is accurate and reliable; laws, regulations, and policies are adhered to; and economy and efficiency are achieved. As such, the IRM Program applies to all programs and functions.

4. Background

a. The Budget and Accounting Procedures Act of 1950 required that each agency head establish and maintain a system of accounting and internal control. The expectation was that such a system would help diminish fraud, waste, abuse, and mismanagement in federal government operations. In August 1980, the Act notwithstanding, the Government Accountability Office (GAO) reported that widespread internal control breakdowns continued to occur in the federal government.

b. As a result of the GAO findings, Congress passed reference (a) in September 1982. The Federal Managers' Financial Integrity Act (FMFIA) mandates that each executive agency's internal accounting and administrative controls be established per standards prescribed by the Comptroller General. In reference (b), the GAO provides the standards for internal control in the government. Further, the Act requires that the Office of Management and Budget (OMB), in consultation with the GAO, publish guidelines for agencies to use in establishing, maintaining, evaluating, improving, and reporting annually on their internal control systems. The OMB guidelines are spelled out in reference (c). An annual Statement of Assurance (SOA), or Certification Statement, from the head of each executive agency is submitted to the President and Congress. It attests to the agency's efforts to comply with the requirements of the Act. The statement must describe the agency's significant accomplishments (if required), material internal control weaknesses or significant deficiencies (if applicable), if any, and corrective action plans (if applicable).

c. Reference (d) provides implementation policy and guidance to the Secretary of the Navy's (SECNAV) IRM program which replaced the MICP. The IRM Program is now in the process of being renamed to the Risk Management and Internal Control (RMIC) Program. Reference (e) requires commands to implement a system of documented internal controls to provide reasonable assurance that the following objectives are met: (1) Effectiveness and efficiency of operations; (2) Reliability of financial reporting; and (3) Compliance with applicable laws and regulations. This requirement encompasses all programs and functions within the Navy, not just the comptroller functions of budgeting, recording, and accounting for revenues and expenditures. Managers are required to incorporate basic

internal controls into the strategies, plans, guidance, and procedures governing their programs and operations. SECNAV requires that internal controls be reviewed annually with the results reported via the annual SOA certification statement.

5. Discussion

a. The Department of the Navy (DON) IRM Program is the Navy's method for demonstrating and documenting compliance with FMFIA. SECNAV expects all managers to be active participants. During audits and inspections, external agencies (GAO, Department of Defense (DoD) Inspector General, Naval Inspector General, and Naval Audit Service) may review command compliance with this program. During NETC command inspections, compliance with the IRM Program will be reviewed. See reference (f) for guidance concerning the Command Inspection Program.

b. The NETC IRM Program also stresses using a variety of existing methods to gauge the effectiveness, efficiency, and economy of work processes (WP) or assessable units (AU). A process is defined as the manner in which resources are employed in generating a product, performing a responsibility, or rendering a service in support of the Navy’s mission. It consists of starting and ending points that are connected by a series of decision points and various work-related steps. Strategically located throughout the process should be key metrics (performance indicators) for gauging how well the process is performing.

c. Specifically, internal controls (management safeguards) are the organization, policies, and procedures used to reasonably assure:

(1) Programs and operations achieve intended results in support of command strategic goals and objectives.

(2) Resources are used consistent with the Navy's mission.

(3) Programs and resources are protected from fraud, waste, and mismanagement.

(4) Laws and regulations are followed.

(5) Reliable and timely information is obtained, maintained, reported, and used for decision making.

d. SECNAV stresses that internal controls are to be integrated into the daily practices of all managers, and must:

(1) Encompass all operations and mission responsibilities of an organization.

(2) Not be duplicative of existing information that pertains to evaluating the effectiveness of internal controls.

(3) Be advocated and supported by organizational leadership.

(4) Identify, report, and correct material weaknesses and significant deficiencies. These are instances where internal controls are not in place, not used, or not adequate. The attention of the next higher level of management is required.

6. Relationship of the Command Evaluation (CE) Program to the NETC IRM Program. Reference (g) provides NETC policy and guidelines for conducting internal reviews. The NETC CE Program is a disciplined in-house method for performing independent reviews of activity operations and processes. It is a proactive mechanism for internally detecting and correcting a condition that may adversely impact mission, command integrity, or the economical use of resources. It may also be utilized as a preparatory tool for NETC command inspections. During in-house reviews, internal controls should be routinely evaluated for adequacy. Where warranted, CE recommendations are directed to the appropriate manager for corrective action. The individual performing the review is not responsible for establishing, maintaining, or improving internal controls. This falls under management's purview. The CE Program also includes the NETC audit liaison roles and responsibilities.

7. Relationship of Immediate Superior in Command Oversight and NETC Command Inspection Program to the NETC IRM Program. The NETC IRM Program is the foundation for the NETC Command Inspection Program. Reference (f) provides the guidelines for performing a command inspection. By completing the process analysis associated with the NETC IRM Program, a command can also simultaneously prepare for a command inspection. This approach

allows the command to stay in a perpetual state of readiness for any inspection, review, or audit. The NETC IRM Program can give a command an effective mechanism to quickly gauge the health of a process with a minimum investment of time and effort.

8. Relationship of Operational Risk Management (ORM) to the NETC IRM Program. ORM involves identifying and assessing process hazards (risks or vulnerabilities) and implementing controls to reduce the risk associated with any process operation. Guidelines for the ORM process are discussed in reference (h). An operation should be continuously monitored for effectiveness of controls and situational changes. The WP and AU flowcharts, developed through the NETC IRM Program, provide a solid framework for assessing risks and evaluating the effectiveness of controls. With the inclusion of key metrics, the flowchart is a useful tool for pictorially displaying pulse points, which permit a rapid preliminary evaluation of various aspects of risk. This method allows the manager to identify and isolate risky areas very quickly. Consequently, managers are able to make better informed decisions about how best to reduce the severity of risk.

9. Definitions. IRM Program definitions are discussed in enclosure (1).

10. Policy. It is the policy of NETC that all NETC HQ and domain activities develop, implement, maintain, review, and improve accounting and administrative controls. On an ongoing basis, all commands must be vigilant concerning the adequacy of internal control systems. All levels of management must comply with the guidelines of this instruction. Per reference (d), NETC (including NETC HQ and domain) will establish an independent IRM team or office, led by the IRM Coordinator, that has direct access to the Executive Offices.

a. The IRM Coordinator and Alternate IRM Coordinator will be appointed (in writing) by their commander, CO, or director (as applicable). Echelon 2 commands must have full-time IRM coordinators and IRM coordinator duties must be identified on their position descriptions (PD) (if civilians), or formal job duties (if active duty). Active duty IRM coordinators or alternates must also be appointed using the IRM Coordinator Appointment Letter template in reference (d). Echelon 3 and their subordinate commands are not required to have full-time IRM coordinators or alternates. Their IRM coordinators or

alternates must have an appointment in writing, either via their PD (if civilian), or the IRM Coordinator Appointment Letter template. If NETC domain civilian IRM coordinator duties are not cited on their PDs, they must also use the IRM Coordinator Appointment Letter template to be appointed as IRM coordinator or alternate. No IRM coordinators will be located in the Inspector General or Comptroller Offices. IRM coordinators are responsible for the administration and coordination of the IRM Program to align with the reporting requirements of the FMFIA.

b. NETC HQ and domain activities will appoint, in writing, AU Managers (AUM), via the AUM Appointment Letter template in reference (d). AUMs must be appointed by the commander, CO, or director (as applicable). AUMs must be military or civilian employees serving in leadership positions that serve as process level managers for their assessable units. They are responsible for assisting the IRM coordinator by providing oversight of their business processes or assessable units and administering the IRM Program to align with the reporting requirements of the FMFIA.

c. NETC HQs and domain activities will appoint, in writing, AU Representatives (AURs), via the AUR Appointment Letter template in reference (d). AURs are appointed by AUMs. AURs must be military or civilian employees. They are responsible for assisting the RMIC coordinator and AUM in RMIC reporting requirements.

11. Roles and Responsibilities

a. NETC will facilitate the implementation of an effective governance process to establish and maintain compliance with noted policy and Chief of Naval Operations (CNO) guidance.

b. IRM Coordinators will:

(1) Provide IRM oversight and the establishment of an effective governance process to ensure that NETC HQ and the NETC domain is adhering to all policies and procedures.

(2) Analyze, compile, and coordinate signature of the annual IRM SOA certification statement.

(3) Identify best business practices and recommend ways to improve control documentation, enhance controls, eliminate inefficient controls, or implement new controls.

(4) Ensure identified efficiencies, "best practices," and deficiencies are shared within the command.

(5) Review assessments.

(6) Assist AUMs and process owners or managers to:

(a) Establish risk management practices to identify and manage risks related to mission-support and other operations as determined by management.

(b) Identify internal control objectives based on risk assessment.

(c) Perform self-assessments of organizations and core business lines, identifying deficiencies and developing corrective action plans (CAP), including milestones to correct deficiencies.

(7) Maintain documentation (such as process flows and narratives, associated risk matrices, control objectives, control activities, and SOA certification statements) from AUMs that will assist in the completion of IRM requirements such as operational process flows, narratives, risk documentation, testing, and certification statements.

(8) Liaise with the Director, Navy Staff (DNS)-F5 Internal Control Office for Internal Control Over Reporting deficiencies related to operational, financial, and systems processes.

(a) Communicate with the DNS-F5 Internal Control Office and appropriate IRM governance body regarding any deficiencies identified through internal assessments that may impact the commands' level of assurance over its internal control environment or a DON-level deficiency or strategic initiative.

(b) Monitor and track CAP implementation for material weaknesses listed in the SOA certification statement.

(9) Complete applicable internal control or IRM training as defined by CNO and as directed per reference (d).

(10) Ensure the command's AUs and WPs are reviewed annually and updated by cognizant managers.

(11) Ensure AUs and WPs are flowcharted (to include key metrics) and internal control system tests (ICST) and ORM assessments have been performed.

(12) Ensure risk assessments and internal control evaluations are completed, as required by CNO.

12. Procedures. To ensure NETC documents risks and evaluates internal controls to mitigate those documented risks, the following annual procedures are required:

a. Segment the Activity and Assign Responsibilities

(1) Categorize command WPs and AUs into a WP inventory that reflects mission critical and associated support processes. For each process, ensure that a responsible manager is identified.

(2) Based upon mission and associated support, commands may have significantly different inventories. To evaluate the WP and AU, develop, at a minimum, a one-page mid-level linear flowchart. The flowchart should depict the process from start to finish. An important by-product of a flowchart is the identification of two to three key metrics (performance indicators) that permit routine testing for effectiveness, efficiency, and economy. Documentation must be retained in-house for turnover and audit or inspection purposes. It also supports the requirement for performing process self-assessments in preparation for NETC command inspections.

(3) The flowchart defines how the process works. It shows interrelationships with other processes, as well as redundancies. Internal control points are displayed in the form of process and decision steps, which serve as prime measuring points. Each point becomes a quality indicator that can be quickly assessed for efficiency, effectiveness, and economy. This assessment provides a picture of risk and vulnerability to internal control breakdowns. This characteristic of the flowchart also affords a

non-subject matter expert an opportunity to make a reasonable assessment. Ultimately, this approach permits the command leadership an opportunity to swiftly evaluate command processes. For this reason, flowcharts are invaluable turnover tools.

b. Strategic Goals, Key Metrics, ICST, and ORM Assessment

(1) Ensure each process is examined for efficiency, effectiveness, and economy. Each process should be tied to a command strategic goal or objective. Identify the two to three key metrics that can be used to measure performance. For ready reference, ensure the locations of the key metrics are clearly annotated on the process flowchart. These metrics should provide a quick look as to how well a process is progressing in achieving its intended purpose.

(2) Ensure internal control evaluations are conducted for mission critical, associated support, and universal work processes. The ICST (NETC 5200/1) is used by NETC to document internal control testing. Internal controls provide reasonable assurance that the objectives of the program and process are achieved. They are (1) designed to mitigate risks; (2) ensure what should occur in daily activities does occur on a continuing basis; and (3) ensure processes are working as desired, reduce error, and identify problems as they occur. Additional internal control evaluation methodology is also required by CNO and DNS-F5.

(3) Under the guidelines of reference (h), ensure an ORM assessment has been performed for mission critical, associated support, universal WPs and any process deemed high risk. ORM involves identifying and assessing process hazards (risks and vulnerabilities) and implementing internal controls to reduce the risk associated with any process. NETC requires the use of the ORM Assessment (NETC 5200/2) to provide a streamlined format for completing a risk assessment. Additional risk assessment methodology is also required by CNO and DNS-F5.

(4) Ensure annual ICST and ORM assessment forms are properly attested to, signed, and dated by the appropriate individuals.

c. Annual IRM SOA Certification Statement

(1) To demonstrate the existence of a clear audit trail of accountability at the activity level, department heads must submit a signed annual SOA certification statement to the commander, CO, or director. The reporting cycle runs from 1 October through 30 September.

(2) Echelon 2 commands must submit their final (signed) SOA certification statement which includes a consolidated risk assessment, internal control evaluation, and CAPs (if applicable), to the DNS and DNS-F5 by 30 April.

(3) Each fiscal year, NETC must complete a required risk assessment and internal control evaluation using the "ICE Risk Assessment Tool." Input to the tool populates the risk assessment spreadsheet and template which is an enclosure to the SOA certification statement. This risk assessment spreadsheet identifies and categorizes risks related to significant operational and financial areas or programs that leadership deems as critical to achieving mission objectives, and that may impact the quality of data that management relies on for operational decision making. It assesses the identified risks by applying a risk rating criterion to evaluate the overall exposure to the risks associated with the operational area, and documents the command's risk response strategy.

(4) Echelon 3 commands must submit a consolidated statement that reflects chain of command compliance by both echelon 3 commands and their subordinate commands. Commanders and COs reporting directly to NETC must provide electronically a signed SOA certification statement along with applicable enclosures to the NETC IRM Coordinator for compilation.

13. Action

a. Heads of Activities

(1) Comply with the policies and procedures set forth in this instruction.

(2) Ensure that all responsible managers actively participate in the IRM Program and that their participation is considered during annual performance evaluations.

(3) Ensure that appropriate training is provided to responsible managers and IRM Program coordinators.

b. Activities Reporting Directly to NETC. Complete the above actions and the following:

(1) Ensure appropriate managers evaluate field level reports pertaining to their area of responsibility and alert other cognizant commands of unusually good or bad conditions reported.

(2) Ensure planned actions for correcting material weaknesses or significant deficiencies are completed in a timely manner.

(3) Assess program compliance at subordinate commands.

14. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned per the records disposition schedules located on the DON Assistant for Administration, Directives and Records Management Division portal page at https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx.

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact the local records manager.

15. Review and Effective Date. Per OPNAVINST 5215.17A, NETC will review this instruction annually around the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, DoD, SECNAV, and Navy policy and statutory authority using OPNAV 5215/40 (Review of Instruction). This instruction will be in effect for 10 years, unless revised or cancelled in the interim, and will be reissued by the 10-year anniversary date if it is still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the need for cancellation is known following the guidance in OPNAV Manual 5215.1 of May 2016.

16. Forms. The following forms are available for download from the NETC public web site (www.netc.navy.mil). Other IRM templates and forms will be provided by the NETC IRM Coordinator.

a. NETC 5200/1 (Internal Control System Test (ICST))

b. NETC 5200/2 (Operational Risk Management (ORM) Assessment)

J. J. CZERWIEC

Releasability and distribution:
This instruction is cleared for public release and is available electronically on the NETC public web site (www.netc.navy.mil) or by e-mail at netc-directives@us.navy.mil.

DEFINITIONS

1. Assessable Unit (AU). To support its control environment, the DON has structured itself into AUs or subdivisions to appropriately define strategic objectives and business processes, implement and assess internal controls, and provide adequate oversite and management for each of the DON's core functions. AUs are identified based upon the programs, processes, administrative activities, or functions significant to mission accomplishment.

2. Assessable Unit Manager (AUM). The AUM must be a military member or government civilian with the knowledge of daily operations of an AU. The AUM can be appointed by either the commander, CO, or director (as applicable) or the RMIC coordinator. AUMs serve as the action-level managers of AUs who support RMIC coordinators fulfilling IRM program requirements and oversee the processes within their AU's purview.

3. Assessable Unit Representative (AUR). The AUR must be a military member or government civilian serving within an organization supporting the efforts of an AUM. The AUR is appointed by the AUM and supports all AU activities. The AUR communicates regularly with the appropriate command's RMIC coordinator.

4. Business Process Operations. The activities, processes, functions, interfaces, automation, or communication performed to achieve a specified objective or combination thereof:

a. The summation of all efforts expended in achieving a defined objective apart from unique classifications supporting the entity's (e.g., component, AU) functioning such as reporting.

b. Business process operations may be further classified to characterize the nature of those business process operations such as administrative, financial, engineering, production, logistical, maintenance, safety, public relations, or information technology (IT) performed for an entity (e.g., component, AU, combat support operations entity (to include supply, logistics, financial support, medical support, maintenance, but not including military warfighting operations).

5. Control Activities. Ensures management directives are carried out. They are the policies, procedures, techniques, and mechanisms that enforce management's directives and provide reasonable assurance that actions are taken to address risks. Control activities are an integral part of an entity's planning, implementing, reviewing, and accountability for stewardship of government resources and achieving effective results.

6. Corrective Action Plans (CAP). AUMs are to evaluate findings from both self-reported issues and external audits and reviews, determine proper actions in response to self-reported findings and recommendations from audits, and complete, within the established time frames, all actions that correct or otherwise resolve the matters brought to management's attention. This documentation can and should be used to back up the annual SOA certification statement.

7. Deficiencies. Deficiencies are results from assessments, inspections, evaluations, audits, or any other type of review. These results indicate non-compliance to instructions or policies.

8. Documentation. Documentation of internal control activities is required to the extent needed by managers (military and civilian) to control operations effectively, and to evaluate the comprehensive nature of their programs. IRM documentation is mandated by reference (c), and must include:

a. Inventory of AUs.

b. Risk Assessments.

c. Internal Control Assessments.

d. CAPs (if applicable).

Note: Documentation can also include process narratives; flow charts; organizational charts; and quarterly status on corrective actions. Key supporting documentation must be maintained, per this instruction, for subsequent review by management and inspector general or audit personnel.

9. Findings. Findings are results from assessments, inspections, evaluations, audits, or any other type of review. These are process improvement recommendations.

10. Integrated Risk Management (IRM) Coordinator. IRM coordinators must be military members or government employees serving in leadership positions that serve as the command's focal point, disseminating guidance and procedures to fulfill the intent of the IRM Program. IRM coordinators are appointed by their CO or head of command.

11. Internal Assessments and Reviews. An impartial and objective appraisal or verification of data, procedures, and performance of operations, systems, activities, programs, functions, and internal controls. Internal assessments are conducted to determine if command resources are managed properly and in compliance with laws and regulations; command programs are achieving their objectives and desired outcomes; and command services are being provided efficiently, economically, and effectively. Internal assessments also help management identify risks and develop process improvement initiatives. Internal assessments are conducted by the Command Evaluation Officer or their designee.

12. Internal Control. An integral component of an organization's management process that provides reasonable assurance that the following is being achieved: effectiveness and efficiency of operations, reliability of reporting for internal and external use, and compliance with applicable laws and regulations. Internal controls are the plans, methods, and procedures used to meet missions, goals, and objectives. Internal controls are the first line of defense in safeguarding assets and preventing and detecting errors and fraud. Internal controls are not single events, but a series of actions and activities that occur throughout operations on an ongoing basis.

13. Internal Control Assessment (Test). A documented evaluation on the effectiveness and adequacy of the internal control system to provide reasonable assurance that mission objectives will be achieved.

14. Material Weakness (MW) – Criteria. A MW exists when a condition results in a relatively high risk of loss, errors, or irregularities in relation to the assets or resources being

managed. Professional judgment, based on applied common sense, must be used when determining materiality. A MW is an internal control deficiency that the agency head determines to be material enough to report outside the agency due to its impact and likelihood or potential impact and likelihood to mission, resources, or image. It warrants the attention of the next level of leadership or command, either to act or for awareness. "Material to the DON" is the final determination of whether a material weakness is to be included in the annual SOA certification statement.

15. Non-compliance. A nonfulfillment or failure to meet a requirement as specified by governing policies, procedures, laws, or customers.

16. Process Owner or Manager. The person within an AU who directs and manages the activities associated with a specific process.

17. Risk. A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action (e.g., the establishment of internal controls). Risk is classified as either low, moderate, or high.

18. Significant Deficiency (SD). Similar to a MW, the SD materiality level designation is a management judgment decision on an issue that warrants senior leadership visibility and resolve for remediation. SDs are often differentiated from MWs in terms of their overall severity on the organization and level of action outside and above the organization's leadership or command needed; SDs are considered by management as detrimental to objective completion, but internally manageable and remediable. An internal controls over operations (ICO) SD is an operational control or a combination of operational control deficiencies that adversely effects the organization's ability to satisfy its mission or be compliant with relevant laws, regulations, and policies, or both. The SD inhibits effective and efficient business process operations and performance reporting.

19. Statement of Assurance (SOA). This statement (also known as Certification Statement) documents risks and internal controls via the Risk Assessment and Internal Control Evaluation

Summary enclosures and can include key financial, operational, and IT system internal controls and risks that are part of a command's primary business operations. It attests to the level of assurance that internal controls have been assessed and evaluated and can also include MW or SD and associated CAPs (if applicable).