DEPARTMENT OF THE NAVY
BUREAU OF MEDICINE AND SURGERY
7700 ARLINGTON BOULEVARD
FALLS CHURCH, VA 22042

IN REPLY REFER TO
BUMEDINST 5200.13B
BUMED-M81
27 Sep 2016

BUMED INSTRUCTION 5200.13B

From: Chief, Bureau of Medicine and Surgery

Subj: MANAGERS' INTERNAL CONTROL PROGRAM

Ref: (a) Federal Managers' Financial Integrity Act of 1982, P.L. 97-255
(b) OMB Circular A-123
(c) DoD Instruction 5010.40 of 30 May 2013
(d) SECNAVINST 5200.35F
(e) SECNAV M-5200.35
(f) OPNAVINST 5200.25E
(g) GAO-14-704G, Standards for Internal Control in the Federal Government
(h) GAO-01-1008G, Internal Control Management and Evaluation Tool
(i) SECNAVINST 7000.27B
(j) BUMED ltr 5200 Ser M82/11UM82757 of 5 Jan 2012
(k) BUMED ltr 5200 Ser M82/14UM80787 of 6 Oct 2014

Encl: (1) Definitions
(2) Acronyms
(3) Senior Management Council and Executive Oversight Group) for Internal Controls
(4) Risk Assessment Guidance - Internal Controls Over Non-Financial Operations
(5) Components of Effective Internal Control Accomplishment or Deficiency Write-up
(6) Sample Appointment Letter – Managers' Internal Control Program Coordinator
(7) Generic Assessable Unit Questionnaire - Internal Controls Over Non- Financial Operations

1. Purpose. To improve accountability in achieving the Navy Medicine mission by implementing an effective internal control program. To provide resources in references (a) through (k) to evaluate and improve operational and business processes. To support a commitment to integrity, ethical values, competence, and accountability in performance by providing updated guidance to Bureau of Medicine and Surgery (BUMED) activities for developing and maintaining effective internal controls (IC).

2. Cancellation. BUMEDINST 5200.13A.

3. Scope and Applicability. BUMED activities at every echelon are responsible for maintaining a positive system of ICs and must follow the general IC guidance set forth in this instruction. However, BUMED will provide annual fiscal year Managers' Internal Control Program (MICP) guidance that identifies the activities required to establish a formal MICP. Those activities identified in the annual fiscal year MICP guidance must follow the specific MICP requirements set forth in this instruction.

4. Background

a. Reference (a), implemented by executive agencies through reference (b), articulates the responsibility of all federal managers to establish and maintain an effective system of ICs over their programs. A properly developed and maintained system of ICs enhances a manager's ability to execute programs effectively and efficiently, provide reliable financial reports and comply with laws and regulations. The safeguarding of assets from unauthorized acquisition, use, and disposition is a subset of all IC objectives.

b. The MICP requires managers to assess ICs over their program areas, report any material weaknesses, and implement appropriate corrective actions. Per references (c) and (d), the MICP is a single, integrated program that promotes a robust system of ICs. The MICP has three parallel and complementary components:

(1) Internal Controls Over Non-Financial Operations (ICONO) provide structure for program managers to monitor program, operational, and administrative ICs over all processes within BUMED. ICONO objectives are met through functional area and/or program assessments, deficiency identification, root cause analysis, and corrective action implementation.

(2) Internal Controls Over Financial Reporting (ICOFR), as detailed in Appendix A to reference (b), is specifically concerned with ICs over key processes that impact BUMED's financial statements and supports financial improvement and audit readiness efforts. ICOFR objectives are met through transaction testing, deficiency identification, root cause analysis, and corrective action implementation.

(3) Internal Controls Over Financial Systems (ICOFS), as detailed in Appendix D of reference (b), are specifically designed to evaluate the control environment and analyze risks that impact BUMED's assurance over the ability of the integrated financial management systems (IFMS) in use to produce reliable and timely financial information. ICOFS testing supports compliance with the Federal Financial Management Improvement Act of 1996 and the Federal Information System Controls Audit Manual (FISCAM). BUMED does not own any of the financial management systems that are utilized on a daily basis and, therefore, relies heavily on the operational and systems controls assessments conducted by system owners. However, as a system user, BUMED is responsible for the operating effectiveness of complementary user entity controls (CUECs). ICOFS objectives are met through CUEC assessments covering areas such as system access and segregation of duties.

c. The BUMED MICP incorporates reporting requirements from the Defense Health Agency and the Department of Navy (DON). Reference (c) guides reporting from Service Medical Activity-Navy (which includes the Defense Health Program funding received, executed, and reported by BUMED) to the Defense Health Agency. References (d) through (f) guide reporting from BUMED to DON.

d. BUMED will publish annual fiscal year guidance for BUMED activities to guide their MICP efforts for that program year. That annual guidance will identify assessable units (AUs) to be reviewed for the ICONO, ICOFR, and ICOFS components of the MICP. The guidance will outline the sampling and testing methodology that will be used to meet the requirements of Appendices A and D of reference (b). Additionally, the guidance will detail quarterly and annual MICP reporting requirements and other specific instructions.

5. Definitions and Acronyms. Standardized definitions of terminology used in conjunction with the MICP can be found in enclosure (3) of reference (d). BUMED interpretations and clarifications of terminology can be found in enclosure (1) of this directive. Acronyms used in this instruction can be found in enclosure (2).

6. Policy. All BUMED activities, regardless of whether or not they are required by the annual fiscal year MICP guidance to establish a formal MICP, are responsible for establishing ICs throughout their organization that include five standards: control environment, risk assessment, control activities, information and communications, and monitoring. Reference (g) defines the five standards of internal control, as established by the Government Accountability Office (GAO). Reference (h) provides a useful framework for incorporating these requirements into existing business processes. The five standards are:

a. Control Environment. Managers at every echelon within BUMED must fully embrace ICs and create an organizational culture that promotes integrity and ethical behavior. Assessment, implementation, and enhancement of ICs should be a continuous effort, not an isolated response to annual reporting requirements.

b. Risk Assessment. Senior leadership engagement is necessary to establish and promote a risk conscious organization. As defined in enclosure (3), the BUMED Senior Management Council (SMC) and Executive Oversight Group (EOG) for ICs institutionalize enterprise risk management at the BUMED headquarters level. Enterprise risk management will influence decision making at the enterprise level, as well as, IC activities throughout the organization. Additionally, managers at all levels of the organization should regularly conduct risk assessments within their areas of responsibility (AOR). Such assessments help identify areas where the absence of effective ICs poses the greatest risk to mission accomplishment. Managers should consider risks to overall operations, accurate and reliable financial reporting, and compliance with laws and regulations. The following questions may help identify the greatest risks within programs:

(1) What could go wrong in the process?

(2) What processes require the most judgment?

(3) What processes are most complex?

(4) What must go right for proper reporting?

(5) How could we fail to report accurately?

(6) How do we know whether we are achieving our objectives?

(7) What business areas are most vulnerable to fraud, waste, and abuse?

Note: When conducting a risk assessment, managers should consider the likelihood and impact of a hazard or misstatement, the likelihood an IC would detect or prevent a hazard or misstatement, as well as the potential materiality of the hazard or misstatement. Enclosure (4) provides guidance on how to conduct a risk assessment for ICONO program areas and/or AUs.

c. Control Activities. ICs should be incorporated into every business process and information system at every echelon of BUMED. The organization, policies, and procedures that constitute IC systems should be formally documented to ensure their continuity, consistency, and effectiveness. Heads of activities and managers are strongly encouraged to highlight essential ICs when issuing local instructions, directives, and guidance (e.g., including a checklist of property accountability ICs in a command personal property instruction). ICs should further, not hinder, mission accomplishment. Managers should ensure that the benefits of implementing an IC outweigh the cost and ensure an appropriate balance between too many and too few controls. Key internal control categories include:

(1) Top-level and management reviews.

(2) Management of human capital (e.g., human capital strategy is in place; employee roles and responsibilities are well-defined and tied to the organization's mission; skilled and competent employees are recruited; employees receive orientation, tools, and training to perform their jobs effectively; employees have necessary credentialing).

(3) Information processing (e.g., system edit checks, access controls over data).

(4) Physical control over vulnerable assets (e.g., cash audits, physical inventories of supplies, disaster recovery plans, sensitive assets such as information technology equipment kept in secure locations).

(5) Performance measures and indicators (e.g., metrics are established and monitored, variances from plan are analyzed).

(6) Segregation of duties in place to prevent conflict of interest and reduce the risk of error, waste, or fraud.

(7) Transaction authorizations and approvals.

(8) Recording of transactions and events (e.g., transactions are completely, accurately, and properly recorded, maintained, and supported by documentation and audit trails).

(9) Access restrictions and accountability for resources and records

d. Information and Communications. Personnel at all levels need to maintain awareness of management goals, legal and regulatory guidelines, and changes to operating environment. IC systems should be adapted accordingly.

e. Monitoring. Monitoring the effectiveness of ICs should occur through the normal course of business, with an emphasis on high-risk programs. On a fiscal year basis, BUMED will specify methodologies for ICONO, ICOFR, and ICOFS assessments at the entity, region, and activity level, which may include sampling and testing transactions. To monitor ICs, in addition to ICONO, ICOFR, and ICOFS AU reviews, managers must use management reports, risk/opportunity assessments, Federal Information Security Management Act reviews, legal reviews (including Anti-Deficiency Act investigations), Inspector General (IG) inspection reports, anti-fraud input from IG staff, notice of findings and recommendations from Financial Statement Examinations/Audits, site assist visit results, and external audits. Based on the results of IC monitoring activities, BUMED activities, as required by the annual fiscal year MICP guidance, must prepare and submit quarterly certification statements and an annual Statement of Assurance (SOA), certifying the degree to which ICs are operating effectively across their AOR. The certification should be based on reasonable assurance, not absolute assurance. Ultimately, when preparing their quarterly certification statements and annual SOA, managers must consider ICs at all subordinate activities within their AOR, whether or not these activities administer a formal MICP. Additional details regarding reporting requirements will be provided as part of annual fiscal year MICP guidance. The quarterly certification statements and annual SOA must meet the following criteria:

(1) Adhere to the established reporting period:

(a) Quarterly Certification Statements. The quarterly certification statements will cover the ICONO, ICOFR, and/or ICOFS assessments conducted during the quarter. The specific due dates will be provided in the annual fiscal year MICP guidance.

(b) Annual SOA. The annual SOA will cover the time period from 1 July of the previous fiscal year through 30 June of the current fiscal year. All BUMED activities required by the annual fiscal year MICP guidance to submit an annual SOA will include ICs reviewed during the fourth quarter of the prior fiscal year, as well as, ICs reviewed during the first three quarters of the current fiscal year. If a deficiency is identified after the SOA is signed, but before the reporting period closes, and if it remains an uncorrected deficiency, it should be included in the next year's SOA. The annual SOA will normally be due within the first 2 weeks of May of the current fiscal year. The specific due date will be provided in the annual fiscal year MICP guidance.

(2) Include management's separate assertion (unqualified, qualified, or no assurance) for each component of the MICP (i.e., ICONO, ICOFR, and/or ICOFS) assessed during the reporting timeframe.

(3) Document sources of internal control data used to determine the levels of assurance. Only those sources that were used should be listed. The sources may include but are not limited to: ICONO, ICOFR, ICOFS AU assessments; external audits (e.g., Financial Statement Examination/Audit NFRs, Naval Audit Service (NAVAUDSVC), GAO, Joint Commission, etc.); Department of Defense (DoD), DON, Medical IG (MEDIG) inspection reports; site assist visits; informal testing; program reviews (e.g., Procurement Performance and Management Assessment Program, Logistics Assist Visits, etc.); and management observation.

(4) Include management's assessment of the extent to which all applicable Navy Medicine Standard Operating Procedures (SOPs) are employed. The assessment should specifically address comptroller, logistics, and pharmacy AORs. Management will explain the basis for the assessment, including, but not limited to, audit preparation testing and site assist activities.

(5) Be signed by the head of the activity or principal deputy and the Comptroller, unless specified otherwise in the annual fiscal year MICP guidance.

(6) Identify all ineffective ICs, as appropriate, as well as corrective action plans (CAP) with targeted resolution dates to remediate the ineffective ICs. Ineffective ICs must be properly documented according to the requirements outlined in the annual fiscal year MICP guidance. Supporting documentation for quarterly certification statements may include: ICONO, ICOFR, and/or ICOFS AU assessments and prescribed tools for identifying and tracking control deficiencies and CAPs. Supporting documentation for the annual SOA may include: accomplishment write-ups, deficiency write-ups, and CAPs, a compilation of IC assessment data from sources other than MICP, and SOP compliance. In addition to the annual fiscal year MICP guidance, reference (e) will help activities develop their SOAs. Enclosure (5) may be used as a guide for writing up IC accomplishments and deficiencies.

7. Responsibilities

a. Heads of activities must:

(1) Establish and maintain a positive control environment across his or her AOR.

(2) Require managers at all levels and across all functional areas to establish, evaluate, and improve ICs.

(3) If required by annual fiscal year MICP guidance, establish and maintain a formal MICP within the staff performing the comptroller function for the activity, as an assignment of other responsibilities per reference (i), paragraph 5j. The MICP will monitor and report on ICs within all functional areas across the activity's AOR.

(4) Where a formal MICP is required, appoint, in writing, a government civilian or military member MICP coordinator from within the comptroller staff to execute program responsibilities related to the ICONO, ICOFR, and ICOFS components of the MICP. Whenever possible, an Alternate MICP coordinator should also be appointed. Enclosure (6) contains a sample appointment letter. The MICP coordinator will inform the Comptroller, who must have unfettered access to the head of the activity per reference (i), of any IC issues, as necessary.

(5) Use informed judgment to determine the materiality of all identified control deficiencies. Enclosure (1) defines the different categories of control deficiencies and criteria for materiality. If required to submit an annual SOA by the annual fiscal year MICP guidance, maintain thorough documentation to support a decision to exclude any auditor or IG-identified material weaknesses from the organization's annual SOA.

(6) Assign a senior accountable official responsible for developing and overseeing execution of a CAP for each material weakness reported. The senior accountable official must be a senior DON official at the Flag Officer/Senior Executive Service level. If the activity does not have an official at that rank/grade, the head of the activity will be the senior accountable official and will not further delegate this responsibility. An identified material weakness should not be considered closed until at least one of the following occurs:

(a) An independent review (i.e., audit, IG assessment) confirms that a weakness no longer exists.

(b) A valid IC test based on random sampling and statistical testing confirms that an IC has been implemented and is working effectively.

(c) The reporting activity achieves a pre-established and reported metric.

(d) The function in which the weakness was reported is eliminated or transferred to another activity.

(e) The senior accountable official provides a written declaration that the weakness has been resolved.

(7) Ensure all applicable Navy Medicine SOPs are fully implemented across the AOR, as required by reference (j). If required to submit formal reports by the annual fiscal year MICP guidance, certify the extent to which all applicable Navy Medicine SOPs are employed and the effectiveness of SOP implementation and application in the activity's quarterly certification statements and annual SOA.

(8) If required by the annual fiscal year MICP guidance, sign the activity's quarterly certification statements and annual SOA for submission to higher echelon. In the absence of the head of the activity, the principal deputy may sign.

(9) Provide assistance as needed to other activities, Services, and agencies that identify material weaknesses related to BUMED.

b. Navy Medicine Echelon 3 Commanders must:

(1) Oversee and guide IC assessment and testing efforts at subordinate activities (e.g., military treatment facilities or support activities) within their AORs. These assessment efforts may include random sampling and testing efforts to support ICONO, ICOFR, and ICOFS components of the MICP. Echelon 3 quarterly certification statements and annual SOAs will take into consideration IC assessment and testing results reported by subordinate activities.

(2) Serve as principal members on the SMC for Internal Controls. See enclosure (3) for SMC roles and responsibilities.

c. The Deputy Chief of Business Operations/Comptroller (BUMED-M4/6/8) (echelon 2) and Resource Manager/Comptroller (echelon 3 and below) must:

(1) Serve as the senior advisor to the head of activity on ICs and keep the head of activity informed on all significant IC issues impacting the AOR.

(2) At the echelon 2 level, serve as a principal member on the SMC for IC; the Assistant Deputy Chief of Financial Management (BUMED-M8) will serve as a principal member on the EOG for IC. At the echelon 3 level, serve as an ad hoc member on the EOG. See enclosure (3) for SMC and EOG roles and responsibilities.

(3) At the echelon 3 and below level, if required by the annual fiscal year MICP guidance, sign the activity's quarterly certification statements and annual SOA for submission to higher echelon. In the absence of the Resource Manager/Comptroller, the Deputy Resource Manager/Comptroller may sign.

d. The BUMED MICP Coordinator/Alternate MICP Coordinator (echelon 2) must:

(1) Reside in the BUMED, Financial Management Division (BUMED-M8).

(2) Implement, oversee, and sustain the ICONO, ICOFR, and ICOFS components of the MICP at the enterprise level, administering program responsibilities on a day-to-day basis.

(3) Provide enterprise-wide fiscal year MICP guidance on an annual basis, detailing specific quarterly and annual reporting requirements.

(4) Establish a MICP inventory as part of the annual fiscal year MICP guidance, including required ICONO, ICOFR, and ICOFS AUs. This inventory will be the basis for each lower echelon's fiscal year MICP plan.

(5) Work with AU program managers and/or subject matter experts at the headquarters level to conduct risk assessments and develop AU assessments. Provide AU program managers and/or SMEs with AU assessment results. As necessary, assist AU program managers and/or SMEs with the development of CAPs in response to internal and/or external IC assessment/audit findings.

(6) Provide AU assessment templates, populated with applicable information to support ICONO, ICOFR, and ICOFS efforts, to lower echelon MICP coordinators.

(7) Prepare the enterprise-wide annual SOA per the Chief of Naval Operations and the Defense Health Agency guidance and submit to both organizations.

(8) Brief the SMC and/or EOG, as appropriate, on MICP efforts and facilitate discussions regarding program/functional risk areas, ICs, deficiencies, CAPs, and SOPs.

(9) As necessary, conduct periodic reviews of documentation related to efforts of the ICONO, ICOFR, and/or ICOFS components of the MICP at all organizational levels.

(10) Have MICP responsibilities incorporated into his or her performance appraisal.

(11) Complete the DON Managers' Internal Control Program Training course for coordinators on Navy Knowledge Online upon appointment. The MICP Coordinator and Alternate will also complete refresher training every 3 years after appointment.

e. <u>The MICP Coordinator/Alternate MICP Coordinator (echelon 3 and below) must</u>:

(1) Implement, oversee, and sustain the ICONO, ICOFR, and ICOFS components of the MICP, administering program responsibilities on a day-to-day basis.

(2) Develop and disseminate program guidance and reporting requirements, if needed to supplement the annual fiscal year MICP guidance issued by the BUMED enterprise MICP Coordinator.

(3) Establish a MICP plan on a fiscal year basis, outlining mandatory and elective AUs to be assessed. The MICP plan will follow the requirements provided in the annual fiscal year MICP guidance.

(4) Conduct risk assessments with AU program managers and/or SMEs, following the guidance at enclosure (4) and the annual fiscal year MICP guidance.

(5) Work with AU program managers to develop AUs for any program areas identified as high risk due to absence or ineffectiveness of ICs. Enclosure (7) may be used as a guide for developing an ICONO AU questionnaire.

(6) Review quarterly ICONO, ICOFR, and ICOFS AU results for completeness, ensuring assessments follow the guidance and standards set by the BUMED enterprise MICP Coordinator. If errors, omissions, or misrepresentations of information are found, return assessments for correction, completion, and/or explanation.

(7) Assist AU program managers with the development and implementation of CAPs where ineffective, weak, or nonexistent ICs are identified. Ensure CAPs include targeted resolution dates and monitor CAP implementation to ensure deficiencies are fully corrected or reported to higher echelon when higher level assistance is needed. Where CAPs span multiple activities within the AOR, coordinate planning and implementation of improvement efforts.

(8) Prepare the activity's quarterly certification statements and annual SOA in conformance with the annual fiscal year MICP guidance, based on:

(a) Reviews of mandatory ICONO, ICOFR, and ICOFS AUs.

(b) Reviews of elective AUs.

(c) Other sources of IC data identified in paragraph 6e(3).

(9) Brief quarterly certification statements and the annual SOA to the head of activity and Comptroller. Topics addressed should include, but not be limited to, ICONO, ICOFR, and ICOFS AU results; new IC deficiencies and CAPs; and CAP implementation for existing IC deficiencies.

(10) Maintain documentation for higher-level reviews and audit purposes.

(11) Have MICP responsibilities incorporated into his or her performance appraisal.

(12) Complete the DON Managers' Internal Control Program Training course for coordinators on Navy Knowledge Online upon appointment. The MICP Coordinator and Alternate will also complete refresher training every 3 years after appointment.

f. Financial Improvement and Audit Readiness Teams (echelon 3) must:

(1) Engage with the MICP coordinators at their echelon 3 and BUMED headquarters to further support IC evaluation, deficiency identification, and corrective action implementation.

(2) Analyze results and data from activities in their AOR including, but not limited to, ICOFR and ICOFS testing and remediation, Audit Assertion Testing, site assist visits, documentation requests, and Financial Statement Examination/Audit findings.

(3) Prioritize and correct, as appropriate, IC deficiencies. Any deficiencies that warrant reporting should be included in the annual SOA of the appropriate Navy Medicine echelon 3 activity.

g. The SMC and EOG for IC (echelon 2) must:

(1) Follow the roles and responsibilities outlined in enclosure (3).

(2) Provide a forum for discussing, assessing, and monitoring MICP efforts to include: program/functional risk areas, ICs, deficiencies, CAPs, and SOPs.

(3) Coordinate and discuss IC and financial improvement actions resulting from, but not limited to: MICP; Financial Statement Examination/Audit; Department of Defense, DON, and MEDIG inspection findings and best practices; external audits such as NAVAUDSVC and GAO; and Military Health System Review findings.

h. BUMED Directorates (echelon 2) must: Support CAP implementation and collaborate with BUMED-M8 to issue new or revised policies that will bring internal controls within specific programs, financial areas, or systems into compliance with established laws and regulations.

i. MEDIG must:

(1) Ensure BUMED activities comply with this instruction.

(2) Consult with management as needed on IC assessments. The MEDIG will not conduct IC assessments on behalf of program managers.

(3) Provide inspection findings and best practices to the BUMED enterprise MICP Coordinator as required in reference (k).

(4) Provide Anti-Fraud annual report to the BUMED enterprise MICP Coordinator.

(5) Serve on the SMC and EOG for ICs in a consulting capacity as required by enclosure (3).

8. Information Control Management. Reports on the MIC Program have been assigned Report Control Symbol DD-COMP (A) 1618 per paragraph 6 of reference (c).

TERRY J. MOULTON
Acting

Releasability and distribution:
This instruction is cleared for public release and is available electronically only via the Navy Medicine Web site at: http://www.med.navy.mil/Pages/default.aspx

DEFINITIONS

1. AU. A programmatic or functional area capable of being evaluated by internal control assessment procedures. The AU should be small enough to provide reasonable assurance of adequate ICs and large enough to detect any material weaknesses that would have a potential impact on Navy Medicine's mission. BUMED publishes annual fiscal year guidance identifying the AUs each required MICP reporting entity will review for the MICP year. Heads of activities and managers may use local risk assessments to develop elective AUs, as a supplement to mandatory AUs.

2. Assessable Unit Program Manager. The individual responsible for the oversight and monitoring of internal controls related to a specific assessable unit.

3. CUEC. Internal controls that a system user is responsible for implementing and overseeing to ensure transactions are properly authorized and executed prior to transmission to an external service organization. System owners may assign CUECs to the system user at the entity level.

4. Control Deficiency. A condition in which the absence, design, implementation, or operation of a control does not allow management or employees (in the normal course of performing their assigned functions) to prevent or detect fraud, waste, abuse, mismanagement, or misstatement in a timely manner. Control deficiencies may be categorized as follows:

a. ICONO

(1) Material Weakness. A reportable condition, or combination of reportable conditions, that adversely affects the ability to meet mission objectives and is deemed by the head of the activity to be significant enough to report to the next higher level. Material weaknesses must be reported to the next higher level in the activity's Annual SOA. Materiality is a management judgment. Criteria commonly identified with materiality are:

(a) The issue is control-related.

(b) The deficiency threatens mission, resources, or organizational image.

(c) The deficiency exists across the organization.

(2) Reportable Condition. A control deficiency, or combination of control deficiencies, that adversely affects the ability to meet mission objectives, but is not deemed by the head of the activity serious enough to report as a material weakness. Reportable conditions are normally within the organization's ability to correct, are generally not reported outside the organization, and progress of corrective actions is tracked internally.

(3) Item to be Revisited. An internal control issue brought to management's attention with insufficient information to determine whether the control deficiency is material. These issues will be revisited throughout the fiscal year to determine the materiality of the control deficiency.

b. ICOFR and ICOFS:

(1) Material Weakness. A reportable condition, or combination of reportable conditions, that results in more than a remote likelihood that a material misstatement of the financial statements, or other significant financial reports, will not be prevented or detected. The determination of a weakness's materiality is a management judgment.

(2) Reportable Condition. A control deficiency, or combination of control deficiencies, that adversely affects the ability to initiate, authorize, record, process, or report external financial data reliably per Generally Accepted Accounting Principles. There is more than a remote likelihood that a misstatement of the financial statements, or other significant financial reports, is more than inconsequential and will not be prevented or detected.

(3) Internal Control Deficiency. Exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements in a timely manner.

5. CAP. A written document that describes the specific steps necessary to resolve a control deficiency, including targeted milestones, completion dates, and accountable parties responsible for implementing the milestones. Milestones should be:

a. Specific: Define the scope of the problem, avoid being broad and describe clear actions that will be taken to fix the deficiency.

b. Measurable: Identify and quantify completion criteria and results for each milestone.

c. Achievable: Corrective actions should be within the reporting organization's capacity and its existing resources to implement. It must be noted in the CAP if the reporting organization depends on another organization to take action.

d. Realistic: Corrective actions should be within the reporting organization's existing resources to complete. Corrective actions requiring new resources must be included in future budget requests.

e. Time-bound: Time milestones so they may be implemented properly and within realistic expectations.

6. FISCAM. The FISCAM provides a methodology for performing effective and efficient information system controls audits, either alone or as part of a performance audit, a financial audit, or an attestation engagement, including communication of any identified control weaknesses. FISCAM is consistent with National Institute of Standards and Technology's guidelines for complying with the Federal Information Security Modernization Act of 2014.

7. Head of Activity. Commander, commanding officer, or officer in charge of an activity.

8. ICOFR. Process to assess program, operational and administrative controls, report control deficiencies, and implement corrective actions across all functional areas within an organization. Only ICs with a potential material impact on financial reporting are reviewed within the ICOFR component of the MICP.

9. ICONO. Process to assess program, operational and administrative controls, report control deficiencies, and implement corrective actions across all functional areas within an organization. ICs within the ICONO component of the MICP are reviewed without regard for potential impact on financial reporting.

10. ICOFS. Process to assess the control environment and analyze risks that impact a manager's assurance over the ability of the IFMS in use to produce reliable and timely financial information. Assessments allow for the identification, reporting, and correction of control deficiencies.

11. Levels of Assurance

a. Unqualified. Reasonable assurance that ICs are effective with no material weaknesses reported or that the IFMS are in conformance with federal requirements. Certification must be accompanied by a firm basis for this position.

b. Qualified. Reasonable assurance that ICs are effective with the exception of one or more material weaknesses or the IFMS is not fully compliant with federal requirements. Certification must cite material weaknesses that precluded an unqualified statement.

c. No Assurance. No reasonable assurance that ICs are effective because few or no assessments were conducted, the noted material weaknesses are pervasive across many key operations, or the IFMS is substantially noncompliant with federal requirements.

12. Materiality. The threshold above which a deficiency/error could prevent the organization from accomplishing mission objectives or reporting reliable financial data for management to use in the decision making process. Some factors to consider when determining the appropriate severity level of the deficiency/error are the following: impact on mission success or failure;

health and safety; threat to image; pervasiveness throughout the organization; and/or management's reliance on the financial data impacted. The level of materiality becomes more significant as a deficiency/error has a greater impact on those factors.

13. Reasonable Assurance. An informed management judgment regarding the overall adequacy and effectiveness of ICs to deter or detect material failures based upon available information that the systems of ICs are operating per Financial Managers' Financial Integrity Act objectives. There is a high degree of confidence but not absolute confidence.

14. Risk. The possibility an event will occur and adversely affect the achievement of objectives. Risk assessment is the identification and analysis of risks related to achieving the defined objectives to form a basis for designing risk responses.

15. Root Cause Analysis. A focused analysis of a deficiency or exception to determine why it occurred and what action needs to be taken to correct it.

16. Senior Accountable Official. A DON manager at the Flag Officer/Senior Executive Service level who is appointed, in writing, to oversee prompt resolution of a material weakness an activity identifies in its annual SOA.

ACRONYMS

AOR	Area of Responsibility
AU	Assessable Unit
BUMED	Bureau of Medicine and Surgery
CAP	Corrective Action Plan
CUEC	Complementary User Entity Control
DON	Department of the Navy
ERM	Enterprise Risk Management
EOG	Executive Oversight Group
FISCAM	Federal Information System Controls Audit Manual
GAO	Government Accountability Office
IC	Internal Control
ICOFR	Internal Controls Over Financial Reporting
ICOFS	Internal Controls Over Financial Systems
ICONO	Internal Controls Over Non-Financial Operations
IFMS	Integrated Financial Management Systems
IG	Inspector General
MEDIG	Medical Inspector General
MICP	Managers' Internal Control Program
NAVAUDSVC	Naval Audit Service
SMC	Senior Management Council
SOA	Statement of Assurance
SOP	Standard Operating Procedure

SENIOR MANAGEMENT COUNCIL AND EXECUTIVE OVERSIGHT GROUP FOR INTERNAL CONTROLS

1. Objective. The objective of the Navy Medicine SMC and EOG for IC is to provide senior management oversight and accountability for non-financial, financial reporting, and financial systems operations. To meet this objective, focus areas must include, but not be limited to, enterprise risk management (ERM), IC assessment, and risk mitigation.

2. Reference. Provisions for an SMC are set forth in the Office of Management and Budget (OMB) Circular A-123, "Management's Responsibility for IC." OMB Circular A-123 defines Federal management's responsibility for IC and provides guidance to Federal managers for establishing, assessing, correcting, and reporting on effective ICs.

3. Purpose. The SMC and EOG are structured to provide executive level oversight to Navy Medicine leadership at the headquarters (echelon 2) and echelon 3 levels on operational and financial management initiatives. The SMC and EOG are not separate, chartered groups; but they will operate under the purview of the chartered Executive Steering Council and Assistant Deputy Chiefs Council, respectively. The SMC and EOG will ensure Navy Medicine's commitment to an appropriate system of internal control tailored to the organization's operational and financial risks. Both groups will be forums for executing ERM and discussing and resolving critical internal control issues related to internal and external audits, program reviews, and management concerns. The SMC and EOG are decision making bodies and have the authority to task.

a. The SMC and EOG must establish and execute ERM. ERM, as defined by the Association for Federal Enterprise Risk Management, is "a discipline that addresses the full spectrum of an organization's risks, including challenges and opportunities, and integrates them into an enterprise-wide, strategically-aligned portfolio view. ERM contributes to improved decision-making and supports the achievement of an organization's mission, goals, and objectives." This portfolio view ensures all areas (e.g., finance, procurement, information technology/information assurance, manpower, medical operations, training) of the organization's exposure to risk are assessed and the appropriate action taken.

b. ERM will be the driver for determining the appropriate channel for non-financial operations, financial operations, and financial systems internal control assessments. Appropriate assessment channels include, but are not limited to: MICP, MEDIG, and the NAVAUDSVC.

c. The SMC and EOG must also focus on identifying and correcting systemic IC deficiencies related to functional areas across the Navy Medicine enterprise (e.g., finance, procurement, information technology/information assurance, manpower, medical operations, training). Sources of IC deficiencies include, but are not limited to: external audit reports (e.g., Department of Defense (DoD) IG, Navy IG, NAVAUDSVC, GAO); MICP assessment reports; Financial Statement Examination/Audit Notice of Findings and Recommendations; MEDIG reports; program reviews; and management concerns.

d. As outlined in OMB Circular A-123, the SMC and EOG must be responsible for: providing input for the level and priority of resources needed to correct IC deficiencies; overseeing the timely implementation of corrective actions related to material weaknesses; and determining when sufficient action has been taken to declare a significant deficiency or material weakness corrected. Both groups will recommend to the Chief, BUMED which IC deficiencies are material to disclose in the annual Federal Managers' Financial Integrity Act SOA on ICs.

4. Structure. The EOG will be a component of the SMC, and all ERM and IC matters will be presented to this group first for discussion and decision. According to the guidelines outlined in the responsibilities sections below, the EOG will provide discussion and decision content to the SMC. The SMC's responsibilities will be executed through the chartered ESC and the EOG's responsibilities will be executed through the chartered Assistant Deputy Chiefs Council.

5. Membership

The SMC will be comprised of:

Team Member	**Membership Role**
Executive Director	Chairperson
Deputy Chief of Total Force	Principal Member
Deputy Chief of Readiness & Health	Principal Member
Deputy Chief of Business Operations/Comptroller	Principal Member
Commander, Navy Medicine East	Principal Member
Commander, Navy Medicine West	Principal Member
Commander, Navy Medicine Education and Training Command	Principal Member
MEDIG	Advisor

The EOG will be comprised of:

Team Member	**Membership Role**
Assistant Deputy Chief of Financial Management (BUMED-M8)	Chairperson
Assistant Deputy Chief of Manpower & Personnel (BUMED-M1)	Principal Member
Assistant Deputy Chief of Education & Training (BUMED-M7)	Principal Member
Assistant Deputy Chief of Research & Development (BUMED-M2)	Principal Member
Assistant Deputy Chief of Healthcare Operations (BUMED-M3)	Principal Member

Assistant Deputy Chief of Operations Medicine and Capabilities, Development, (BUMED-M9)	Principal Member
Assistant Deputy Chief of Fleet Support and Logistics (BUMED-M4)	Principal Member
Assistant Deputy Chief of Information Management and Technology (BUMED-M6)	Principal Member
Chief of Staff, Navy Medicine East	Principal Member
Chief of Staff, Navy Medicine West	Principal Member
Deputy Commander, Navy Medicine Education and Training Command	Principal Member
Deputy, MEDIG	Advisor
Ad hoc members: Navy Medicine echelon 3 Comptrollers, Program Managers, Subject Matter Experts	Contributor

6. Meetings.

a. Frequency. The EOG will meet at least quarterly and more frequently as necessary. The SMC will meet at least quarterly, following the EOG meeting, and more frequently as necessary.

b. Decision Making for SMC. The Chairperson for the SMC will make the final decision on all "advice and consent" items discussed in the "SMC Responsibilities" and "Shared Responsibilities" sections below. The Chairperson will also make the final decision on other discussion items as deemed necessary. In making the final decision, the Chairperson will consider input and advisement from the Principal and Advisor Members on the SMC. As the final decision maker, the Executive Director will be accountable for the decision. Final decisions will be distributed to SMC participants via meeting minutes.

c. Decision Making for EOG. The EOG will vote on all "advice and consent" items discussed in the "EOG Responsibilities" and "Shared Responsibilities" sections below. Other discussion items may require a vote as deemed necessary. Each Principal Member, except the Chairperson, must have an equal vote. The Chairperson must only vote in matters of a tie. Items not unanimously agreed to must be decided by a majority vote. Only Principal Members present at the EOG meeting can vote, unless they provide their vote two business days prior to the meeting. Principal members can select a government proxy to vote in their absence. Voting results will be distributed to EOG participants via meeting minutes.

d. Administrative Support. The Financial Improvement and Audit Readiness Division (BUMED-M81) will provide administrative support to both the SMC and EOG. Responsibilities will include but are not limited to: setting meeting agendas; taking and distributing meeting minutes; and providing guidance for ERM, internal control deficiency evaluation, and corrective action plan design.

7. EOG Responsibilities. To achieve the objective and purpose outlined above, the EOG must:

a. Oversee enterprise risk management/assessment:

(1) On an annual basis, prior to the start of the new fiscal year, review risk assessments performed by each M-code. The BUMED enterprise MICP Coordinator will provide specific guidance and a template for the risk assessment. The M-code risk assessments will be the basis for the Enterprise Risk Inventory. The EOG will present the Enterprise Risk Inventory to the SMC, including what is being done to measure, mitigate, and monitor the risks.

(2) Based on the Enterprise Risk Inventory, provide advice and consent on what programs and/or processes should be included in the annual MICP AU inventory, DON Risk and Opportunity Assessment, and MICP annual SOA.

b. Evaluate potentially systemic IC deficiencies and determine if they need to be presented to the SMC for action.

(1) Deficiencies will come from the following inputs/sources (among others):

(a) External audit reports (e.g., DoD IG, Navy IG, NAVAUDSVC, GAO)

(b) MICP Assessment Reports

(c) Financial Statement Examination/Audit Notice of Findings and Recommendations

(d) MEDIG Reports

(e) Joint Commission Reports

(f) Patient Safety Program

(g) Risk Management Program

(h) Unauthorized Commitment Ratifications

(i) Program Reviews (e.g., Procurement Performance and Management Assessment Program, Logistics Assist Visits)

(j) Management concerns

(2) The following considerations will guide the deficiency evaluation and influence whether or not the deficiency is taken to the SMC for action:

(a) What is the issue?

(b) Is the issue related to issues identified in other sources?

(c) What is the risk level associated with the issue?

(d) Who will fix the issue?

(e) What resources (e.g., funding, manpower) are needed to fix the issue?

(f) When will the issue be fixed?

(3) Based on the deficiency evaluation, deficiencies will go to the SMC for action based on the following criteria:

(a) There is uncertainty over the answers to the questions in paragraph 7b(2) (i.e., unable to assign responsibility for correction, unable to determine when the issue will be fixed or deadlines are repeatedly missed, unable to identify and/or implement an effective corrective action).

(b) Issues identified as high risk.

(c) External dependencies for issue correction.

(d) External and/or higher level policy or law requires revision in order for Navy Medicine to comply and the issue to be resolved.

(e) Lack of resources for correction.

c. For IC deficiencies remaining at the EOG level, take the following actions as necessary:

(1) Prioritize corrective actions.

(2) Approve proposed corrective action plans.

(3) Ensure adequate resources (e.g., funding, manpower) are available to implement approved corrective action plans.

(4) Assign responsibility for corrective action.

(5) Oversee the timely implementation of corrective actions.

(6) Determine when sufficient action has been taken to declare an IC deficiency corrected.

(7) Determine the deficiency severity (e.g., item to be revisited/control deficiency, reportable condition, or material weakness) and whether or not the deficiency should be reported in Navy Medicine's MICP Annual SOA.

d. For all IC deficiencies, track corrective action plan implementation status.

8. SMC Responsibilities. To achieve the objective and purpose outlined above, the SMC must:

a. Review the Enterprise Risk Inventory provided by the EOG. Provide advice and consent on the Enterprise Risk Inventory and on what programs and/or processes should be included in the annual MICP AU inventory, DON Risk and Opportunity Assessment, and MICP Annual SOA.

b. Review IC deficiencies brought forward by the EOG and take the following actions:

(1) Where there is uncertainty regarding the deficiency evaluation, determine the appropriate action (i.e. who is responsible for correction, set and/or enforce corrective action deadlines, determine and/or enforce an effective corrective action plan, etc.).

(2) Where high risk issues are identified, determine the appropriate corrective action, the deficiency severity (e.g., item to be revisited/control deficiency, reportable condition, or material weakness) and whether or not the deficiency should be reported in Navy Medicine's MICP Annual SOA.

(3) Where there is dependency on external parties/agencies for correction, engage with the party/agency if appropriate to determine a mutually agreeable solution. Ask DON and/or DHA for assistance if needed/appropriate.

(4) Where external and/or higher level policy or law precludes Navy Medicine compliance, engage with DON and/or DHA for assistance.

(5) Where there is a lack of resources to implement a corrective action, determine what resources are needed (e.g., funding, manpower) and take appropriate action to assign those resources to the corrective action implementation.

(6) Regarding other scenarios, take the following actions as necessary: prioritize corrective actions; approve proposed corrective action plans; assign responsibility for corrective action; oversee the timely implementation of corrective actions; and determine when sufficient action has been taken to declare an IC deficiency corrected.

9. Shared Responsibilities. Both the SMC and EOG will be responsible for the following outputs:

a. Task corrective actions to the appropriate parties, and ensure timely and effective resolution.

b. Provide advice and consent on the Enterprise Risk Inventory.

c. Provide advice and consent for the MICP AU inventory.

d. Provide advice and consent for the MICP Annual SOA content.

e. Provide advice and consent for the DON Risk and Opportunity Assessment.

f. Provide meeting minutes/status updates on corrective actions.

RISK ASSSESSMENT GUIDANCE
INTERNAL CONTROLS OVER NON-FINANCIAL OPERATIONS

1. Department of Defense Instruction 5010.40 requires that a risk assessment be included as part of the MICP process for assessing ICONO.

2. A risk assessment helps identify potential hazards or unwanted actions that might prevent the AU from achieving its objectives. AU program managers are best able to conduct risk assessments on their programs due to their expert knowledge of the program's objectives and challenges. In addition to their program experience and oversight, AU program managers should consider information from IG inspections, external audits, and Anti-Fraud Program Risk Assessment to help identify additional risks. It is recommended that AU program managers work with their Activity's MICP Coordinator to complete the risk assessment.

3. According to OMB Circular A-123, "management should identify internal and external risks that may prevent the organization from meeting its objectives." AU program managers should consider the risks associated with the objective of the AU. Consider the following questions to help identify risks:

a. What is the objective of the AU?

b. What could go wrong that would prevent the AU from meeting its objective?

c. Where are our vulnerable areas?

d. What processes require the most judgment or are the most complex?

e. What must go right for us to meet the objective?

f. How do we know whether we are achieving our objectives?

4. All MICP reporting entities are required to complete the risk assessment section of the ICONO AU Questionnaire. AU program managers must identify three risks that, regardless of likelihood or impact, could prevent the functional area from meeting its identified objectives. The risk assessment includes the following items:

a. Risk – A risk is a potential hazard or unwanted action that might prevent the AU from achieving its objective. Consider risks that are internal to the command (e.g., training, downsizing, managerial responsibilities, etc.) and also risks that are external to the command (e.g., changing technology, new regulations, risk associated with contractors, etc.).

b. Mitigating IC - An IC is a process used by management to help an activity achieve its objectives. ICs help an activity run its operations efficiently and effectively, report reliable information about its operations, and comply with applicable laws and regulations. For each risk

identified, list all ICs that have been implemented to mitigate that risk. You may list multiple mitigating IC for each risk. ICs may be detective in nature (designed to identify that an undesired outcome has occurred) or preventative in nature (designed to stop an undesired outcome from occurring). A periodic reconciliation of a supply inventory against orders and historic usage is an example of a detective control. Locking supplies in a cabinet is an example of a preventative control.

c. Likelihood - [High, Medium, or Low] – Think about the likelihood that the risk will occur in an environment where no internal controls are in place. Based on the likelihood that the risk will occur, assign High, Medium, or Low, following the descriptions provided in the table below:

Likelihood	Description
Low	The risk is unlikely to occur.
Medium	The risk is somewhat likely to occur.
High	The risk is more likely than not to occur.

d. Impact - [High, Medium, or Low] – Identify the significance the risk would have on the objective if it occurred. Based on the impact that the risk would have on the objective if it were to occur, assign High, Medium, or Low, following the descriptions provided in the table below:

Impact	Description
Low	The risk will not substantively impede the achievement of the objective.
Medium	The risk will cause some elements of the objective to be delayed or not be achieved.
High	The risk will cause the objective to not be achieved.

e. Control Risk - [High, Medium, or Low] – This is the risk that the IC will not mitigate against the identified risk as intended. This is a measurement of the perceived effectiveness of the IC. The following table provides a brief description of the three levels of control risk:

Control Risk	Description
Low	Controls will prevent or detect any hazard or aggregate misstatements that could occur.
Medium	Controls will more likely than not prevent or detect any hazard or aggregate misstatements that could occur.
High	Controls are unlikely to prevent or detect any hazard or aggregate misstatements that could occur.

Example 1: Pharmacy employees taking office supplies home for personal use is identified as a potential risk. The likelihood is assessed as "high" while the impact is assessed as "low." Due to the low dollar value of office supplies purchased and management not having time to monitor how every pencil and paper clip is used, the only control in place is an annual review of the total amount spent on office supplies. The Control Risk is "medium."

Example 2: Pharmacy employees taking narcotics home for personal use is identified as a potential risk. The likelihood is assessed as "medium" while the impact is assessed as "high." The pharmacy conducts a weekly physical inventory of all narcotics and reconciles that inventory against filled prescriptions and manufacturer turn-ins and assigns that control a Control Risk of "low."

COMPONENTS OF EFFECTIVE INTERNAL CONTROL
ACCOMPLISHMENT OR DEFICIENCY WRITE-UP

1. Ensure all accomplishments and deficiencies are IC related. Accomplishments reported in the annual SOA may include: program enhancements to the MICP, actions taken within programs that enhanced internal controls, or control deficiencies that were identified and corrected during the fiscal year reporting period.

2. Report all accomplishments and deficiencies from your organization's perspective. If a subordinate activity reports a deficiency to you, don't simply forward it up the reporting chain. Consider whether that deficiency is really a deficiency for your organization as a whole. If it is, describe the deficiency and report it accordingly. If it isn't, don't report it, but **internally monitor resolution of the deficiency**.

3. Consolidate accomplishments and deficiencies reported by subordinate activities, if it makes sense to do so. If three subordinate activities each report an identical deficiency related to an AU, consider reporting all three as a single deficiency for your organization. Again, **internally monitor resolution of the deficiency** at all three subordinate activities.

4. Be succinct.

5. Provide enough detail so that the accomplishment or deficiency gets sufficient higher-level attention. If you report a deficiency that requires higher-level assistance, you need to provide enough detail so that the scope of the issue and the importance of resolving it is clear.

6. If you need higher-level assistance resolving a deficiency, ask for help when you write it up in the quarterly certification statement or annual SOA. What do you need assistance with and from whom?

7. Write up the accomplishment or deficiency so that someone who isn't a subject matter expert will understand. Avoid unnecessary use of technical jargon. Some of the people who read our SOA may have a limited understanding of Navy Medicine. They may not use the automated systems we are talking about. They may not be financial experts. If you don't describe an accomplishment in terms that someone can understand, it won't be appreciated.

8. Spell out acronyms the first time they are used in each accomplishment or deficiency.

9. Make sure any corrective action dates reported for deficiencies are accurate. If the targeted corrective action date has already passed by the time you prepare the quarterly certification statement or annual SOA, no one will know whether the weakness was resolved or the preparer made an error.

10. Quantify results whenever possible. What is the potential financial impact if the deficiency is not fixed? What percentage of our inventory is unaccounted for? How many man hours did we save annually through an accomplishment?

SAMPLE APPOINTMENT LETTER
MANAGERS' INTERNAL CONTROL PROGRAM COORDINATOR

5200
Ser Code/[*serial number*]

From: [*Head of Region/Activity*]
To: [*Coordinator*]

Subj: APPOINTMENT AS [*ECHELON 3/ACTIVITY*] MANAGERS' INTERNAL CONTROL PROGRAM (MICP) COORDINATOR

Ref: (a) SECNAVINST 5200.35F
(b) BUMEDINST 5200.13

1. Effective this date you are hereby appointed Coordinator of the [*echelon 3/activity*] MICP. You will be guided in the performance of your duties by the provisions of references (a) and (b). Your responsibilities in this capacity will include:

a. Advocating the MICP and internal controls oversight throughout the [*echelon 3/activity*] area of responsibility.

b. Providing recommendations and updates to the command on internal control issues.

c. Providing program support and guidance to subordinate activities within the [*echelon 3/activity*] area of responsibility.

d. Ensuring all MICP reporting requirements are met in a timely manner.

e. Preparing the [*echelon 3/activity*] Annual Statement of Assurance.

f. Monitoring completion of corrective actions on all weaknesses identified to [*higher echelon to which activity immediately reports*] by [*echelon 3/activity*].

g. Completing the "Managers' internal control Program Training for Coordinators" (on Navy Knowledge Online) within 30 calendar days of this appointment and every 3 years thereafter.

h. Notifying the organization of MICP training opportunities and ensuring MICP Coordinators within the area of responsibility are current with training requirements.

2. This appointment is valid until rescinded.

[*Signature block*]

GENERIC ASSESSABLE UNIT (AU) QUESTIONNAIRE
INTERNAL CONTROLS OVER NON-FINANCIAL OPERATIONS

The annual fiscal year MICP guidance will specify requirements for elective AUs. However, activities may develop their own AUs outside of the MICP requirement. The AUs should be mission-specific. Use the questions below as an example when developing assessment questions:

- Does the command have a current SOP and/or instruction for the program?
- Is there a monitoring system in place to assess compliance with applicable SOP/or instructions? If yes, describe the monitoring system.
- Are there accurate position descriptions on file for each program staff position?
- Are program staff responsibilities adequately defined and understood?
- Are education and training resources adequate to provide program staff with the appropriate level of training?
- Are personnel properly assigned according to their level of training and experience?
- If required, are personnel properly appointed to their program management position?
- Do personnel have access to all referenced materials?
- What are the strengths of the program?
- What are the program problems or weaknesses?
- What are the inherent risks in the program?
- Is there a mechanism for identifying areas of potential misuse?
- What preventive, detective, and corrective controls are in place to ensure compliance and efficiency, and prevent fraud, waste, and abuse?
- Is separation of duties in place for inherently high-risk transactions or functions?
- How often are surveys conducted?
- Are random checks conducted to monitor compliance?
- Are there routine inspections or exercises to ensure personnel have knowledge regarding specified situations?
- How often are internal reviews conducted?
- Have there been any external reviews or audits completed in this area? When? By whom (e.g., GAO, Navy IG, Naval Criminal Investigative Service, NAVAUDSVC, etc.)? What were the findings?
- Does the command have performance metrics to monitor the success of the program?
- Is a plan coordinated with local and civilian agencies?
- Are there backup deployment systems in place in case of emergencies?