MANAGEMENT'S RESPONSIBILITY FOR INTERNAL CONTROLS AND REPORTING REQUIREMENTS

COMDTINST 5200.10A
November 2022

THIS PAGE INTENTIONALLY BLANK

U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

US Coast Guard Stop 7710
2703 Martin Luther King Jr. Ave SE
Washington, DC 20593-7710
Staff Symbol: CG-85
Phone: 202-372-3445

COMDTINST 5200.10A
02 NOV 2022

COMMANDANT INSTRUCTION 5200.10A

Subj: MANAGEMENT'S RESPONSIBILITY FOR INTERNAL CONTROLS AND REPORTING REQUIREMENTS

Ref:
(a) Federal Managers' Financial Integrity Act (FMFIA) of 1982, 31 U.S.C. § 3512, Pub. L. 97-255
(b) Office of Management and Budget (OMB) Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, July 15, 2016
(c) Government Accountability Office (GAO), Standards for Internal Control in the Federal Government (the "Green Book"), GAO-14-704G
(d) Chief Financial Officer (CFO) Technical Authority, COMDTINST 5402.3 (series)
(e) DHS Internal Control Playbook, Fiscal Year edition
(f) Coast Guard Executive Management Council Audit, Risk, and Compliance (EMC-ARC) Charter. Memorandum signed by VCG March 25, 2022
(g) Department of Homeland Security Financial Accountability Act (DHS FAA) of 2004, 31 U.S.C. §3516 Pub. L. 108-330
(h) Federal Financial Management Improvement Act (FFMIA) of 1996, 31 U.S.C. § 3512 Pub. L. 104-208
(i) DHS Sensitive Systems Policy Directive 4300A, Version 13.1, July 27, 2017
(j) Government Accountablity Office (GAO), Federal Information System Controls Audit Manual (FISCAM), GAO-09-232G
(k) DHS, Office of CFO Risk Management and Assurance Division (RM&A), Internal Control Playbook and Internal Controls over Financial Reporting (ICOFR) Process Guide, Fiscal Year edition
(l) Memoranda of Understanding/Agreement, COMDTINST 5216.18 (series)

1. PURPOSE. This Commandant Instruction provides policy and information related to meeting the requirements of Reference (a) as interpreted by Reference (b), and guided by Reference (c). The content of this Commandant Instruction is intended to direct Coast Guard managers regarding their responsibility to, through their active involvement, establish, maintain, review, improve, assess, and report on the effectiveness of internal controls within their respective organizations.

2. ACTION. All Coast Guard unit commanders, commanding officers, officers-in-charge, deputy/assistant commandants, and chiefs of headquarters staff elements shall comply with the provisions of this Instruction.

3. AUTHORIZED RELEASE. Internet release is authorized.

4. DIRECTIVES AFFECTED. Management's Responsibility for Internal Control, COMDTINST 5200.10 is hereby cancelled.

5. BACKGROUND. Internal controls are essential to effective management of organizations. They comprise the plans, methods, and procedures employed by managers to meet missions, goals, and objectives, and in doing so, support performance-based management. Internal controls also serve as the first line of defense in safeguarding assets and preventing and detecting errors and fraud, which aids in the effective stewardship of public resources.

   a. The proper stewardship of public resources is an essential responsibility of the Federal Government. To develop and maintain adequate stewardship, federal employees must operate and utilize federal programs and resources efficiently, effectively, and consistent with agency missions. Furthermore, all levels of management must involve themselves in continuous monitoring, assessment and improvements of internal controls.

   b. Internal controls should provide reasonable assurance over operations, reporting, compliance, and the safeguarding of assets. However, an internal control system cannot provide absolute assurance that all of an organization's objectives will be met, nor the absence of waste, fraud, and mismanagement, but it is a means of managing risk associated with programs and operations. Therefore, managers must carefully consider the appropriate balance between risks mitigated by controls and the costs associated with their implementation.

   c. Reference (b) requires agencies to implement a comprehensive management control program, establish governance bodies to provide appropriate oversight, and provide an annual statement of assurance (SOA) over their internal controls, attesting to:

      (1) Effectiveness and efficiency of operations;

      (2) Reliability of financial reporting; and

      (3) Compliance with applicable laws and regulations.

   d. Reference (d) provides technical authority to the Assistant Commandant for Resources/Chief Financial Officer (CFO), Commandant (CG-8), to set the Coast Guard's policy for the establishment, operation, evaluation and improvement of management controls throughout the Coast Guard.

   e. This Instruction provides direction to Coast Guard managers involved in the establishment and maintenance of a robust internal control system in accordance with all applicable references.

6. DISCLAIMER. This guidance is not a substitute for applicable legal requirements, nor is it itself a rule. It is intended to provide operational guidance for Coast Guard personnel and is not intended to, nor does it impose, legally-binding requirements on any party outside the Coast Guard.

7. MAJOR CHANGES. This Instruction has been updated to align with Department of Homeland Security (DHS) and Office of Management and Budget (OMB) guidance and introduces new aspects of internal controls, updated regulations, and re-distributed responsibilities across the enterprise.

a. Standards specific to the internal control program have been removed from the Coast Guard Enterprise Risk Management and Annual Statement of Assurance Reporting Requirements, COMDTNOTE 5200, and included in this Instruction. These standards include identification of Assessable Organizational Elements (AOEs); and the requirement that AOEs report to the Commandant an explicit level of assurance over the effectiveness and efficiency of control activities under their supervision. Additionally, the Statement of Assurance (SOA) reporting timeline has been standardized and summarized in this Instruction.

b. References (f), (g), (e), and (k) have been added to outline the Coast Guard's responsibility to assess internal controls in accordance with DHS' requirements and methodologies. The Internal Controls Assessment Cycle was updated and Requirements to monitor Third-Party Service Providers were added to reflect the procedures outlined in Reference (k).

8. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS. The Office of Environmental Management, Commandant (CG-47) reviewed this Commandant Instruction and the general policies contained within, and determined that this policy falls under the Department of Homeland Security (DHS) categorical exclusion A3. This Commandant Instruction will not result in any substantial change to existing environmental conditions or violation of any applicable federal, state, or local laws relating to the protection of the environment. It is the responsibility of the action proponent to evaluate all future specific actions resulting from this policy for compliance with the National Environmental Policy Act (NEPA), other applicable environmental requirements, and the U.S. Coast Guard Environmental Planning Policy, COMDTINST 5090.1 (series).

9. DISTRIBUTION. No paper distribution will be made of this Instruction. An electronic version will be located in the Coast Guard Directives System Library internally, and if applicable on the Internet at www.dcms.uscg.mil/directives .

10. PROCEDURE. Related procedures and supplemental guidance can be found in on the Commandant (CG-85) CGPortal Page: https://cgportal2.uscg.mil/units/cg85/SitePages/Home.aspx.

11. RECORDS MANAGEMENT CONSIDERATIONS. Records created as a result of this Instruction, regardless of format or media, must be managed in accordance with the records retention schedules located on the Records Resource Center SharePoint Online site: https://uscg.sharepoint-mil.us/sites/cg61/CG611/SitePages/Home.aspx .

12. DISCUSSION. A carefully constructed, utilized, and monitored internal control program is key to achieving the Coast Guard's strategic objectives, and bolstering public trust the Coast Guard.

a. Internal Controls. Internal controls are important to every aspect of the mission, managed by our front-line supervisors. Additionally, internal controls can be witnessed in nearly all aspects of Coast Guard activities. An integral system of internal controls is expected to be applied to both Mission Operations and Financial Accountability in three distinct areas of internal control: Operations, Reporting and Compliance. Operationally, the Assessment, Inspection and Audit (AIA) program identifies critical processes and conducts inspections and audits throughout the Coast Guard. Coast Guard Assessment, Inspection, and Audit Governance, COMDTINST 5040.6 (series) establishes an AIA Configuration Control Board (CCB) and AIA Compliance Oversight Board (COB) to establish accountability across internal control activities specifically

exempting financial and property audits governed by Commandant (CG-8) and any external assessments, audits or inspections which are directed by, and implemented by, an external authority. Financially, controls are documented (in-part) in the Financial Resources Management Manuals for Policy and Procedures, COMDTINST 7100.3 (series) and COMDTINST 7100.4 (series), respectively, and assessed utilizing the framework presented in this Instruction.

b. Governance. Reference (b) requires agencies to establish governance bodies to provide appropriate oversight of the management control program. The Department of Homeland Security (DHS) Risk Management and Assurance (RM&A) Division directs components such as the Coast Guard in providing governance, risk management, and quality assurance over internal controls. Annually, DHS RM&A publishes their annual internal control plan, Reference (e), which provides leadership with DHS' internal control priorities. To comply with applicable references, assure the achievement of Coast Guard objectives, and implement the DHS RM&A internal control plan, the Coast Guard established the below governance and oversight bodies:

   (1) Executive Management Council – Audit, Risk, Compliance (EMC-ARC). The EMC-ARC is an executive advisory body in accordance with the Commandant's Executive-Decision Making (EDM) Process, COMDTINST 5420.40 (series). The EMC-ARC charter, Reference (f), provides direction to executive level oversight and guidance for the Coast Guard's financial audit activities and internal control program.

   (2) Senior Assessment Team (SAT). Under the direction of the EMC-ARC, the SAT works collaboratively to lead Coast Guard efforts to assure accuracy and reliability of reporting, effectiveness and efficiency of operations, compliance with applicable laws and regulations, and financial management systems' conformance with government-wide requirements. The SAT was chartered by the Assistant Commandant for Resources/ Chief Financial Officer (CFO), Commandant (CG-8), as the financial reporting execution arm of the EMC-ARC, responsible for overseeing coordination of key process remediation and development of the Commandant's annual Statement of Assurance (SOA).

   (3) Internal Control Working Group (ICWG). The ICWG was established by the SAT and is a forum which coordinates and implements the activities and responsibilities of their respective SAT representatives to support the successful execution of the annual internal control assessment and coordinate remediation of noted deficiencies. The group's efforts are coordinated by the Office of Internal Controls, Commandant (CG-85).

c. Management. While all levels of management are responsible for internal controls, a risk-based, top down approach is the most effective and efficient method to establish management oversight over internal controls. This approach allows management to focus their attention and efforts on the risks that address the potential sources of material misstatement or pose the highest risks. This level of management is known as an Assessable Organizational Element (AOE).

   (1) Assessable Organizational Elements (AOEs). AOE selection is derived from FMFIA (Reference (a)), Section 2, commonly referred to as Section 2 of the Integrity Act. AOEs are designated levels of management. Typically, these are Flag/SES-led organizations which manage a material amount of risk. AOEs are required to report to the Commandant annually an explicit level of assurance over the effectiveness and efficiency of control activities under

their supervision and direction including financial and non-financial business processes. Furthermore, Reference (a) requires that the Commandant's assurance statement assert or deny reasonable assurance that Coast Guard controls are achieving their intended objectives, and report the existence of material or significant control weaknesses. Such control weaknesses, or exceptions to assurance, are those whose negative consequence would:

(a) Merit the attention of the Executive Office of the President and the relevant Congressional oversight committees;

(b) Violate statutory or regulatory requirements;

(c) Impair fulfillment of essential operations or missions; and/or

(d) Deprive the public of needed services.

(2) AOE Designations. AOE designations are derived from designations made by the EMC-ARC charter (Reference (f)), and further defined below:

(a) AOEs are EMC-ARC member organizations, as designated by the EMC-ARC Charter.

(b) Furthermore, Deputy Commandant for Operations (DCO), Deputy Commandant for Mission Support (DCMS), CG LANTAREA, CG PACAREA and direct reports to the Vice Commandant (VCG) are considered Senior AOEs.

(c) EMC-ARC member organizations who report to the Senior AOEs listed above in paragraph (b), are considered subordinate AOEs.

(3) AOE Remediation. Control deficiencies must be evaluated and remediated by AOEs on a timely basis. Issues that may not be remediated because of the interests of management, such as sensitive information regarding fraud or other illegal acts should be reported to the oversight body. Management override of controls provides the opportunity to commit fraud, circumvents existing control activities, and is prohibited.

13. COMPONENTS OF INTERNAL CONTROL. To achieve an assessment process that relates to external financial reporting and compliance with laws and regulations that have a direct and material effect on financial reporting, DHS and the Federal Government at large, have adopted, in part, standards developed by the Commission of Sponsoring Organizations of the Treadway Commission (COSO) Integrated Framework. DHS holds management responsible for developing and maintaining internal control activities that comply with the five components and 17 principles promulgated by GAO as modified from the original COSO Framework (Figure (1)). To conclude that the design, operation, and implementation of the Internal Control Components are effective, it must be determined that each principle is present and functioning. While the components and principles have a distinct and separate relationship, they do not operate in a vacuum. An effective system of internal control includes Entity Level Controls (ELC) such as fraud prevention, management override policies, risk assessments, tone from the top, and service organization assurances. ELCs, therefore, have a prevalent effect on the internal control system and stretch across many Principles and Components.

Figure 1: Components of Internal Control

GAO Green Book Components	GAO Green Book Principles
Control Environment The foundation for an internal control system. It provides the discipline and structure to help the organization achieve its objectives.	1. Demonstrate Commitment to Integrity and Ethical Values 2. Exercise Oversight Responsibility 3. Establish Structure, Responsibility, and Authority 4. Demonstrate Commitment to Competence 5. Enforce Accountability
Risk Assessment Provides an assessment of the risks facing the organization as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses.	6. Define Objectives and Risk Tolerances 7. Identify, Analyze, and Respond to Risks 8. Assess Fraud Risk 9. Identify, Analyze, and Respond to Change
Control Activities The actions management establishes through policies and procedures to achieve objectives and respond to risks in the internal control system, which includes the organization's information system.	10. Design Control Activities 11. Design Activities for the Information System 12. Implement Control Activities
Information and Communication The quality information management uses to support the internal control system. Communication quality information is vital for an organization to run and control its operations.	13. Use Quality Information 14. Communicate Internally 15. Communicate Externally
Monitoring Activities Assesses the quality of performance over time and ensures that the findings of audits and other reviews are promptly resolved.	16. Perform Monitoring Activities 17. Evaluate Issues and Remediate Deficiencies

14. INTERNAL CONTROLS OVER REPORTING (ICOR). Appendix A of Reference (b) provides a methodology for management to assess, document and report the effectiveness of an internal control system. The Coast Guard has designed an integrated evaluation system and DHS has consolidated reporting requirements into a single report combining Mission Operations, Financial Operations, and Financial Systems.

    NOTE: Mission Operations are assessed within the AIA construct.

    Financially, internal controls can be broken into two areas: Internal Controls over Financial Operations (ICOFO), and Internal Controls over Financial Systems (ICOFS), each relying on the other to establish overall financial integrity. Financial Operations and Systems are assessed as outlined below.

    a. Internal Controls over Financial Operations (ICOFO). Financial operations encompass the scope of Reference (g) to, among other things: design and implement management control activities reflecting the executive strategy, the evaluation of the performance in executing such strategy, and an assertion on the internal controls applicable to the financial reporting. Compliance with

Reference (g) are evaluated in two distinct programs in the Coast Guard's internal control system:

(1) Internal Controls over Financial Reporting (ICOFR). Effective Internal Controls over Financial Operations (ICOFO) requires reasonable assurance regarding the reliability of financial reports and the preparation of financial statements. ICOFR serves as the backbone for providing this assurance and the sustainment of auditable financial statements. If one or more material weakness exists, the organization's internal controls over financial reporting cannot be considered effective. ICOFR is guided by Appendix A of Reference (b).

(2) Internal Controls over (Business) Operations (ICOOPS). The business operations program is designed to identify risks and controls for programs which may not be material, but have specific compliance requirements, are perceived as highly susceptible to fraud, waste, and abuse and can increase reputational risk. Business operations assessed includes, but is not limited to, High Dollar Overpayment (HDOP), Payment Integrity Information Act (PIIA), and the Digital Accountability and Transparency Act (DATA Act). ICOOPS is guided by Appendices A through C of Reference (b).

b. Internal Controls over Financial Systems (ICOFS). Effective Internal Controls over Financial Operations (ICOFO) requires reasonable assurance around the security, protection, confidentiality and integrity of financial data and the availability of the data housed within Coast Guard information systems. ICOFS, also known as information technology (IT) internal controls, provide assurance that Coast Guard financial, mixed, and feeder systems comply with federal financial systems requirements as directed by Reference (h). IT internal controls is guided by OMB Appendices A and D of Reference (b), and OMB Circular No. A-130, Appendix I.

(1) CFO Designated Systems. Annually, the DHS Chief Financial Officer (CFO) provides the Coast Guard with a list of designated IT systems which require additional management accountability to certify that effective internal control exists over financial reporting. Reference (i) establishes departmental policy regarding IT Systems Security and provides a framework for compliance with applicable regulations in regards to CFO Designated Systems. To adequately assess these systems the compliance framework identifies Information Technology General Controls (ITGC).

(2) Information Technology General Controls (ITGC). ITGCs are controls that address structure, policies, and procedures related to an entity's overall computer operations. ITGCs are not tied to any one business process, but may be related to a number of applications, associated technical infrastructure elements, and information systems management organizations that support Line of Business processes. Reference (j) provides guidance on how to incorporate robust and secure financial auditing controls and assess ITGCs such as Security Management (SM), Access Controls (AC), Configuration Management (CM), Segregation of Duties (SD), Contingency Planning (CP), as well as Business Process Application Controls (BPAC).

c. Internal Controls over Third-Party Service Providers. In order to provide assurance over ICOFR and IT systems, management must develop and maintain effective internal controls for activities that are performed by Service Providers and must regularly assess the design and operating effectiveness of the Service Provider internal control environments.

(1) Effective internal controls over the activities performed on behalf of the Coast Guard by the Service Provider provide reasonable assurance that:

(a) Service Providers are appropriately performing activities on behalf of the Coast Guard;

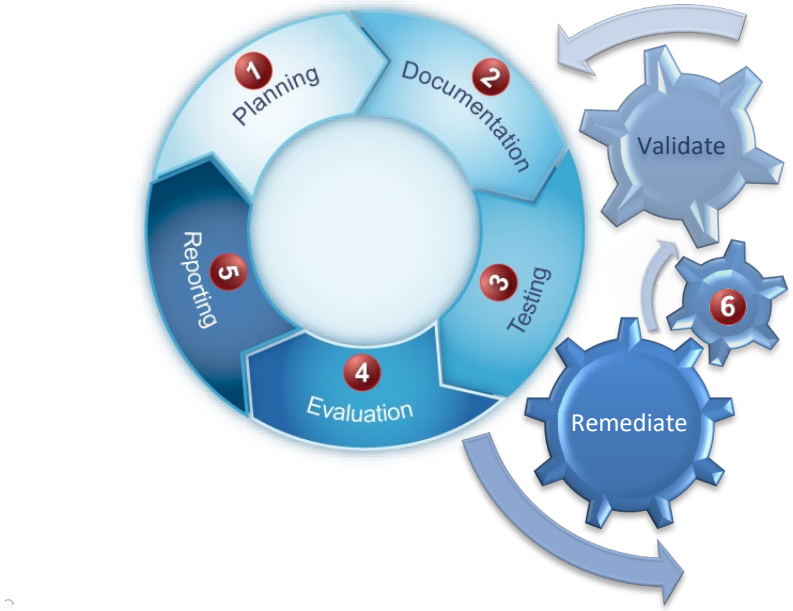
(b) The impact of deficiencies in the Service Providers' control environment are evaluated and the need for compensating controls is determined; and

(c) Complementary User Entity Controls (CUEC) are designed, operating effectively, and periodically reviewed.

(2) Statement on Standards for Attestation Engagements (SSAE) number 18 (Reporting on Controls at Service Providers) defines how entities report on compliance controls; these Service Organization Control (SOC) reports are internal control reports on the services provided and address the risks associated with an outsourced service.

15. INTERNAL CONTROL ASSESSMENT CYCLE. An effective, risk-based approach to assess internal controls is a cumulative, iterative process, not a linear process. It begins at the planning phase, with identifying and understanding areas with higher risk of material misstatement and fraud. It continues with obtaining an understanding of the control environment through discovery and documentation of material processes. Once the risk is understood, the design and implementation of relevant controls are tested. Those results must be thoroughly evaluated and properly reported in a timely manner. The Coast Guard conducts this process continuously throughout the year and may be implementing several phases at once for different internal control areas. It is important to note that every level of management needs to be involved in the execution of the internal control assessment. Assessable Organizational Elements (AOE) are expected to assist in the identification, and provide access to experts in the field, known as Key Process Owners (KPO), who are responsible for each material area. Below are further details and considerations for each of six phases of internal control assessment:

Figure 2: Internal Control Assessment Cycle



a. Planning Phase. Planning is one of the most critical phases in the internal control assessment. It sets the tone for the entire assessment as key processes and control activities are identified and selected to be evaluated throughout the assessment cycle. This phase looks backward and forward: backward to identify the control environment; and forward to determine the scope of the annual assessment. One of the first steps in the Planning Phase is to perform a risk assessment. The risk assessment is a tool that takes into consideration risk tolerance and materiality in order to identify the most significant high-risk processes, financial line items, and the associated entity and process level controls. Plans are then developed to assess control performance; controls addressing high-risk processes and activities are planned for regular testing while lower risk process controls can be evaluated less often.

b. Documentation Phase. Once the risks have been identified, the processes need to be documented. This documentation will form the basis and support for Management's assessment and, in the case of a deficiency, will assist in determining the root cause. Walkthroughs and interviews will assist in the development of process narratives and flow charts which describe the key process areas identified in the planning phase. Supporting documentation is collected to determine whether all applicable risks, control objectives, and financial statement assertions were addressed by the controls. Finally, an assessment of the design and operating effectiveness of key control activities is conducted.

NOTE: **Test of Design (TOD)** is a critical element in assessing a control's planned performance against the objective the control is intended to address. TOD tests a single sample's progress through the entire control process. Factors evaluated include: rigor of control compared to the assessed risk, authority and experience of the process owner, frequency and consistency of the process, and dependencies on other controls.

c. Testing Phase. Controls are tested to make certain: they meet the information processing objectives and related financial statement assertions; they are functioning properly to mitigate risks of material misstatements in the financial reports; and, they support Management's financial reporting assertions. The detailed test plans include identifying controls to be tested, developing testing procedures, and identifying locations for test execution. The plan to test operating effectiveness is centered on control activities that are determined to be designed effectively in the planning and documentation phases.

NOTE: **Test of Effectiveness (TOE)** is an evaluation of the control's actual performance against the designed objective. Process samples are selected and tested to verify the process is operating as it was intended. There are multiple types of testing including inquiry, inspection, observation, and reperformance. The type of testing depends on the risk level of the control activity and the desired level of assurance.

d. Evaluation Phase. An evaluation of deficiencies identified during management's assessment is conducted to determine the magnitude and likelihood of misstatement and the impact to the organization's missions and objectives. Identifying and classifying internal control deficiencies requires a great deal of judgment. Reference (k) provides guidance on identifying, assessing, determining likelihood and magnitude, identifying compensating controls, classifying, aggregating and evaluating deficiencies.

(1) Control Deficiency. A control deficiency exists when the design, implementation, or operation of a control does not allow management or personnel, in the normal course of performing their assigned functions, to achieve control objectives and address related risks. If a reasonable person would conclude, given the possibility of further undetected misstatements, either individually or aggregated, that the misstatement(s) is/are immaterial to the financial statements then control deficiencies are considered to be inconsequential but are still documented during the reporting phase.

(a) Operations, Reporting, and Compliance with Laws and Regulations: Deficiency or minor non-conformity, relating to compliance, operation, and non-financial reporting activities that does not significantly and adversely affect the likelihood that the entity will achieve its objectives.

(b) Financial Reporting: The 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 misstatements on a timely basis.

(2) Significant Deficiency. A significant deficiency exists when a control deficiency or combination of control deficiencies, in management's judgment, adversely affect the ability of the Coast Guard to meet its internal control objectives. This type, or level, of deficiency is less severe than a material weakness; however, if it is at least reasonably possible that a misstatement could occur these deficiencies are considered to be significant and are reported to DHS.

(a) Operations, Reporting, and Compliance with Laws and Regulations: Deficiency or minor non-conformity, or combination of deficiencies, relating to compliance, operation, and

non-financial reporting activities that does significantly and adversely affect the likelihood that the entity will achieve its objectives.

(b) Financial Reporting: Deficiency, or combination of deficiencies, that adversely affect the entities ability to initiate, authorize, record, process, or report financial data reliably such that there is more than a remote likelihood that a misstatement of the entity's financial statements will not be prevented or detected.

(3) Material Weakness. A material weakness exists when a significant deficiency, or combination of significant deficiencies, results in a potential for misstatement which would have been material to the financial statements as defined in the planning stage. When there is a reasonably possible chance of failing to prevent or detect a misstatement which is deemed to be material, control deficiencies are considered to be material weaknesses and are reported to DHS and reported in the Agency Financial Report (AFR).

(a) Operations, Reporting, and Compliance with Laws and Regulations: Deficiency or major non-conformity, or combination of deficiencies, relating to compliance, operation, and non-financial reporting activities that substantially and adversely affects the likelihood that the entity will achieve its objectives.

(b) Financial Reporting: Deficiency, or combination of deficiencies, that results in more is more than a remote likelihood that a material misstatement of the financial statements will not be prevented, detected, and or corrected in a timely manner.

e. Reporting Phase. Timely reporting is critical for addressing control weaknesses and mitigating the associated risk. Because the internal control assessment is iterative and continuous, there are multiple layers of internal and external reporting. Periodically, a Summary of Aggregated Deficiencies (SAD) is prepared which documents the classification of deficiencies. The preparation of the SAD assists with logically evaluating the control deficiencies individually and in aggregate, identifying root causes and trends, and developing corrective action plans. Coast Guard leadership and external stakeholders such as Department of Homeland Security (DHS), Government Accountability Office (GAO), and Office of the Inspector General (OIG) rely on these reports to inform their overall assessment and assurance levels. The reporting phase culminates in the annual Coast Guard Statement of Assurance (SOA) which states management's conclusion on whether the internal controls are effective.

f. Audit and Remediation. Effective remediation of control deficiencies is essential to achieving a mature and sound internal control structure. Correcting deficiencies is an integral part of management accountability and must be considered a priority. Furthermore, Reference (b) requires the establishment of systems to provide prompt and proper resolution and remediation of identified material weaknesses. To facilitate the resolution of internal control deficiencies, DHS implemented a routine monitoring approach (find, fix, test, assert) and issued DHS Management Directive 1030: Corrective Action Plans, and provides a Mission Action Plan (MAP) Guide annually.

(1) Generally, deficiencies which are detected within the internal control assessment cycle and are able to be remediated by Coast Guard managers require a corrective action plan (CAP)

which is approved by the Senior Assessment Team (SAT) and monitored by Commandant (CG-85).

(a) Completion of CAP milestones are tracked and reported on a monthly basis at the SAT meetings.

(b) Upon resolution of the deficiency, the process is placed back into the normal assessment cycle as depicted in Figure (2).

(4) When an external auditor discovers a deficiency, they issue a Notice of Findings and Recommendations (NFR) to the Coast Guard which is reported to DHS. NFR's for enterprise-wide deficiencies requiring significant remediation are addressed by the Coast Guard's Mission Action Plan (MAP) process monitored by Commandant (CG-84).

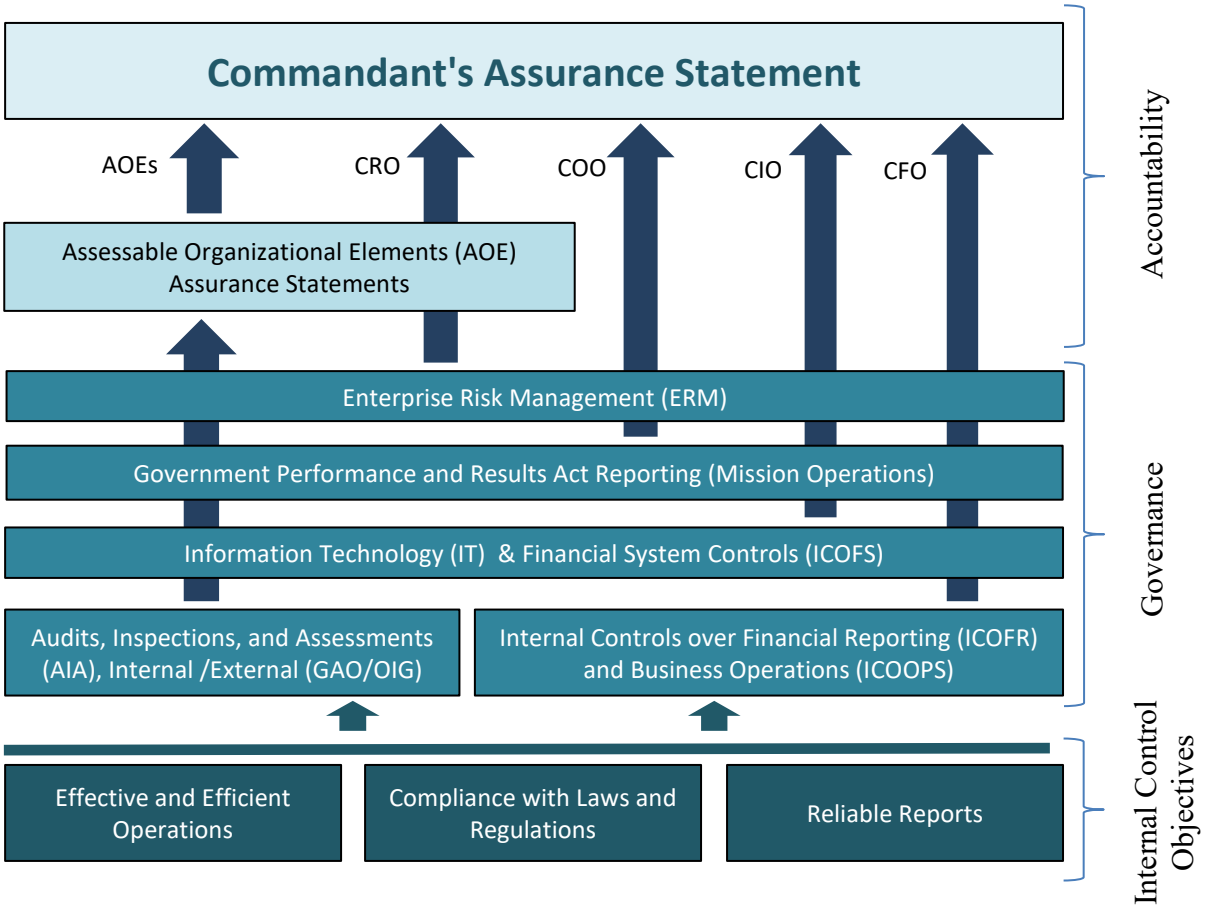
(a) The Mission Action Plan (MAP) is developed during the first fiscal quarter based on DHS prioritization, the prior year's external audit results, and with consideration of internal control assessment findings.

(b) Completion of MAP milestones are tracked and reported on a monthly basis at the SAT meetings.

(c) Once remediation efforts outlined within MAPs are complete, verification and validation (V&V) testing is conducted to confirm that remediation is fully complete.

16. STATEMENT OF ASSURANCE (SOA). The DHS Secretary is required to submit an annual assurance statement related to FMFIA Section 2 (ICOOPs), Section 4 (ICOFS), and DHS FAA (ICOFR) in a single FMFIA report section of the Agency Financial Report (AFR). The AFR is required to be submitted to the President and Congress annually on November 15th. Pursuant to this requirement, DHS sends annual SOA submission guidance to the Coast Guard which includes detailed descriptions of items to be included, the format of the submission, definitions and categories of assurance and a management checklist. Commandant (CG-85) disseminates this guidance through the internal control's governance membership and coordinates efforts to consolidate SOA's from Headquarters Program Managers and Area Commanders representing Assessable Organizational Elements (AOE), Chief Risk Officer (CRO), Chief Operating Officer (COO), Chief Information Officer (CIO) and Chief Financial Officer (CFO) for the Commandant's SOA.

Figure 3: USCG Assurance Statement Reporting



NOTE: While the assurance statement is included as part of the annual Agency Financial Report (AFR), the required assurances are not solely financial. Inputs to the assurance statement derived from non-financial governance activities are coordinated by Commandant (CG-85) with the applicable AOE's during the SOA reporting process.

a. AOE SOA Requirement. Each AOE, as defined in paragraph 11.c is responsible for providing a statement of assurance (SOA), utilizing the AOE SOA template provided in Enclosure (1).

(1) The AOE SOA must provide an attestation to the level of assurance over its internal controls, noting any exceptions to reasonable assurance. "Reasonable Assurance" attests that:

(a) Internal controls are designed to ensure efficient and effective operations, accurate reporting, compliance with laws and regulations, and prevention of misappropriation of assets within their programs; and

(b) AOE's control environment is one that promotes a commitment to integrity and ethical values, a commitment to competence, and the enforcement of accountability in accordance with the applicable GAO internal control standards.

(2) Reporting Timeline:

(a) The Commandant's SOA is due to DHS annually on 30 September;

(b) Senior AOEs, as defined in paragraph 11.c.2.b, are responsible for providing their SOA and all subordinate AOE SOAs to Commandant (CG-8), annually on 30 June;

(c) Subordinate AOEs (direct reports to a Senior AOE) are responsible for providing an SOA to their senior AOE, annually on 15 June; and

(d) All other EMC-ARC member organizations should submit SOA input to their parent AOE, annually on 01 June.

(e) All SOA requirements will be due on the following business day for any due date which falls on a weekend or federal holiday.

(3) Bridge Letter requirements: Although SOA submissions will occur at the end of the third quarter, it is important to gain complete coverage for the year. As such, AOEs which experience any significant changes in the degree of assurance they are able to provide over their internal controls must upgrade or reduce their level of assurance utilizing the Bridge Letter template provided in Enclosure (2).

(a) Bridge Letters are due to Commandant (CG-8) no later than the 15th of September each year.

(b) AOEs who did not experience a significant change in their degree of assurance are not required to provide a Bridge Letter.

b. EMC-ARC SOA Requirement. All AOEs with membership in accordance with the EMC-ARC charter will discuss AOE SOA reporting guidance several times throughout the year, generally following the schedule below:

(1) In Q2, Commandant (CG-8) will brief an overview of the SOA requirements as outlined in the annual DHS guidance.

(2) In Q3 and prior to SOA submission deadlines, Commandant (CG-8) will brief the EMC-ARC to provide additional guidance on making an assurance decision.

(3) In Q4, AOEs will report their findings and SOA determinations.

c. Management's Internal Control Assessment. Assurance over the completion of an AOE's missions and goals cannot be provided pursuant to the internal control assessment cycle alone. Internal controls exist throughout every level of management in the Coast Guard and only the highest risk processes which are material in nature are formally enrolled in the internal control assessment cycle. AOEs are expected to consider the following sources of information for documenting the internal control assessment in their SOA:

(1) Management knowledge gained from the daily operation of agency programs and systems;

(2) Management reviews conducted: expressly for the purpose of assessing the internal control, or for other purposes with an assessment of the internal control as a byproduct of the review, including annual assessments of compliance with laws and regulations and entity level controls;

(3) OIG and GAO reports, including: audits, inspections, reviews, investigations, outcome of hotline complaints, or other products;

(4) Program evaluations, to include results of assessments, inspections, and audits (AIA);

(5) Audits of financial statements conducted pursuant to the Chief Financial Officers (CFO) Act, as amended, including: information revealed in preparing the financial statements; the auditor's reports on the financial statements, internal control, and compliance with laws and regulations; and any other materials prepared relating to the statements;

(6) Reviews of financial systems which consider whether the requirements of the Federal Financial Management Improvement Act of 1996 (FFMIA) and Appendix D of OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, are being met;

(7) Annual evaluations and reports pursuant to the Federal Information Security Management Act (FISMA) and OMB Circular No. A-130, Managing Information as a Strategic Resource;

(8) Annual performance plans and reports pursuant to the Government Performance and Results Act (GPRA) and Government Performance and Results Act Modernization Act (GPRAMA);

(9) Annual reviews and reports pursuant to the Payment Integrity Information Act of 2019 (P.L. 116-117) and Executive Order 13520, Reducing Improper Payments;

(10) Reports and other information provided by the Congressional committees of jurisdiction; and

(11) Other reviews or reports relating to agency operations, including MISHAP reporting.

17. DUTIES & RESPONSIBILITIES. There are a number of Coast Guard offices involved in the execution, monitoring and assessment of internal controls.

a. Office of Internal Controls, Commandant (CG-85).

(1) Develop and communicate specific guidance consistent with this Instruction and relevant DHS, Federal, and Congressional directives;

(2) Provide subject matter expertise, training, and assistance for complying with provisions of this Instruction;

(3) Assess management’s controls for all ICOFO related controls, including ICOFR and ICOOPs, guided by Reference (k);

(4) Provide AOEs with specific guidance and standard templates to fulfill reporting requirements over internal controls;

(5) Conduct verification and validation (V&V) for non-IT remediated processes;

(6) Disseminate annual SOA guidance to AOE's through the SAT and EMC-ARC.

(7) Coordinate the preparation and submission of the AOE SOA's;

(8) Coordinate the preparation and submission of the Commandant's SOA;

(9) Identify Complementary User Entity Control (CUEC) or Compensating Control requirements listed in Third-Party Service Provider's and sub-provider's Service Organization Controls (SOC) reports.

(10) Review and update this Commandant Instruction as necessary for any organizational and systemic changes applicable within the Coast Guard; and

(11) Report results as required by DHS.

b. Office of Cybersecurity Program Management, Commandant (CG-62).

(1) Develop and communicate IT specific guidance consistent with this Instruction and relevant IT DHS, Federal, and Congressional directives;

(2) Provide subject matter expertise, training, and assistance to AOE's for the IT provisions to this Instruction;

(3) Provide an updated systems list to AOEs whenever there are changes to CFO designated systems;

(4) Assess management's controls for all ICOFS related controls as required by Reference (i) and guided by the information technology supplement to Reference (k);

(5) Monitor financial system non-conformances, plans for bringing systems into substantial compliance, and conduct Validation and Verification (V&V) testing for remediated IT processes;

(6) Provide supporting documentation to justify reporting requirements for the annual Coast Guard Statement of Assurance (SOA);

(7) Monitor the remediation of IT related Notice of Findings and Recommendations (NFRs); and

(8) Report results as required by DHS.

c. Office of Financial Policy and Reporting (CG-84).

(1) Develop, monitor, coordinate, and report the Coast Guard Mission Action Plan (MAP); and

(2) Monitor, track, coordinate and report the remediation efforts of Notice of Findings and Recommendations (NFRs).

(3) Monitor verification and validation (V&V) testing over MAPs to confirm that remediation is fully complete.

d. Assessable Organizational Elements (AOE).

(1) Provide the appropriate level of membership to governance councils;

(2) Incorporate internal controls in their strategies, plans, guidance, and procedures that govern their programs, functions, and activities and assess the operating effectiveness of those controls on an annual basis;

(3) Be responsible for reporting on internal controls and compliance with applicable laws and regulations for their respective areas to Commandant (CG-85);

(4) Complete internal control assessment and remediation requirements as directed by Commandants (CG-85), (CG-62), and (CG-84);

(5) Be responsible for the integrity of financial and non-financial data that managers use to manage program activity;

(6) Be responsible for the data input to systems under their ownership and supervision, and the associated internal controls supporting those systems;

(7) Ensure that for all third party service providers where a Service Organization Control (SOC) report is prescribed in accordance with Statement on Standards for Attestation Engagements (SSAE) number 18 (Reporting on Controls at Service Providers), a Memoranda of Understanding (MOU)/Memoranda of Agreement (MOA) exists in accordance with Reference (l), or other appropriate agreement, requiring an independent auditor to perform such an assessment and provide the SOC report to the Coast Guard annually;

(8) Develop Complementary User Entity Controls (CUEC), or compensating controls as required to mitigate risks identified by the SSAE 18 independent auditor;

(9) Produce and retain adequate supporting documentation to support internal control assurances;

(10) Take timely and effective action to correct and document remediation for any identified control deficiency, significant deficiency, material weakness, or audit finding;

(11) Provide an annual assurance statement based on their knowledge and understanding of their organization and relevant supporting documentation provided to them; and

(12) Provide a Bridge Letter to document any changes from the original Statement of Assurance (SOA) through the end of the fiscal year as required. Supporting documentation is required for any changes identified in the Bridge Letter.

18. FORMS/REPORTS. None.

19. SECTION 508. This Instruction adheres to Accessibility Guidelines and Standards as promulgated by the U.S. Access Board. If changes are needed, please communicate with the Coast Guard Section 508 Program Management Office at Section.508@uscg.mil.

20. REQUEST FOR CHANGES. Units and individuals may formally recommend changes through the chain of command using the Coast Guard Memorandum. Comments and suggestions from users of this Instruction are welcomed. All such correspondence may be emailed to Commandant (CG-85) at Internal-Control@uscg.mil.

/STEVEN D. POULIN/
Admiral, U.S. Coast Guard
VICE COMMANDANT

Enclosures: 1. AOE SOA Template
2. AOE Bridge Letter Template

SAMPLE AOE STATEMENT OF ASSURANCE

U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

US Coast Guard
Street Address
City, State, Zip
Staff Symbol:
Phone:

5200
DD MMM YYYY

MEMORANDUM

From: [AOE] Reply to Attn of:

To: [Senior AOE or] Commandant (CG-8)

Subj: FISCAL YEAR XXXX STATEMENT OF ASSURANCE

Ref: (a) Management's Responsibility for Internal Controls and Reporting Requirements, COMDTINST 5200.10 (series)
(b) Government Accountability Office (GAO) 14-704G, Standards for Internal Control in the Federal Government (the "Green Book")

1. In accordance with reference (a), I have directed an evaluation of the control activities within [**AOE**] in effect for the period ending [**DATE**]. The control activities evaluated have been determined to be critical to meeting operational, compliance, reporting, and fraud prevention objectives and are in place to reduce the risk of failing to meet those objectives [**as outlined in enclosure (#)**].

2. Based on the results of this evaluation, including an assessment of applicable items listed in paragraph 15.c of reference (a), [**AOE**] provides **[Reasonable Assurance/Reasonable Assurance with noted exception(s)/No Assurance]** over its internal controls. Furthermore, I provide [**Reasonable Assurance/Reasonable Assurance with noted exception(s)/No Assurance]** that the control environment within [**AOE**] is one that promotes a commitment to integrity and ethical values, a commitment to competence, and the enforcement of accountability in accordance with reference (b).

   a. [(**IF APPLICABLE**) High level summary of noted exception(s). Add additional paragraphs for each exception.]

   b. [(**IF APPLICABLE**) A corrective action plan [attach or describe corrective action plan] has been developed to address any control deficiencies in order to achieve reasonable assurance over internal controls by [**DATE**], [**and is attached in enclosure (#)**].]

3. [(**IF APPLICABLE**) Pursuant to the Digital Accountability and Transparency Act of 2014 (DATA Act), Pub. L. No. 113-101, [**AOE**] provides reasonable assurance that the prime Federal award data submitted to USAspending.gov for publication is correct at the reported percentage of accuracy, and that internal controls that support the reliability and validity of the Component's account-level and award-level data reported for display on

USASpending.gov are achieving their intended objectives, [**except for the following material inadequacy(ies) that was (were) found**:]

a. [(**IF APPLICABLE**) Insert measure name(s) and description(s) of material inadequacy(ies).]

4. [(**IF APPLICABLE**) Pursuant to Management Directive, 112-05, *Home-to-Work Transportation Programs*, [**AOE**] provides reasonable assurance that internal control and reporting over home-to-work transportation is operating effectively, complies with applicable DHS policies and regulations, and achieving its intended objectives**, [except for the following non-compliance(s) that was(were) found**:]

a. [**(IF APPLICABLE**) Insert measure name(s) and description(s) of non-compliance(s).]

5. [(**IF APPLICABLE**) [**AOE**] provides reasonable assurance that the performance data used in the Department's Annual Financial Report, Annual Performance Report, and the Summary of Performance and Financial Information is complete and reliable, [**except for the following material inadequacy(ies) that was (were) found:**]

a. [(**IF APPLICABLE**) Insert measure name(s) and description(s) of material inadequacy(ies).]

6. [**AOE**] provides reasonable assurance that we have implemented an Enterprise Risk Management program. Additionally, our Operational Risk Register has been reviewed, and updated with risk concerns which may significantly impact achieving [**AOE**] missions, goals, or objectives, which I will continue to monitor.

#

Enclosure: Supporting Documentation

Copy: Commandant (CG-85)

SAMPLE AOE BRIDGE LETTER

U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

US Coast Guard
Street Address
City, State, Zip
Staff Symbol:
Phone:

5200
DD MMM YYYY

MEMORANDUM

From: [AOE}

Reply to
Attn of:

To: [Senior AOE or] Commandant (CG-8)

Subj: FISCAL YEAR XXXX STATEMENT OF ASSURANCE

Ref: (a) Management's Responsibility for Internal Controls and Reporting Requirements, COMDTINST 5200.10 (series)

1. In accordance with reference (a), I have conducted an evaluation which notes significant changes to our internal control environment requiring an update our Statement of Assurance.

2. [Summary of changes and the revised level of assurance offered.]

#