



Commandant
United States Coast Guard

US Coast Guard Stop 7618
2703 Martin Luther King Jr. Ave SE
Washington, DC 20593-7618
Staff Symbol: CG-85
Phone: 202-372-3445

COMDTINST 5200.10
18 MAY 2015

COMMANDANT INSTRUCTION 5200.10

Subj: MANAGEMENT’S RESPONSIBILITY FOR INTERNAL CONTROL

- Ref: (a) Federal Managers’ Financial Integrity Act (FMFIA) of 1982, 31 U.S.C. § 3512, (P.L. 97-255)
 (b) Office of Management and Budget (OMB) Circular A-123, Management's Responsibility for Internal Control, Revision Sep 2013
 (c) Standards for Internal Control in the Federal Government, GAO-14-704G, Revision Sep 2014
 (d) Federal Information System Controls Audit Manual (FISCAM), GAO-09-232G, Revision Feb 2009
 (e) Chief Financial Officer (CFO) Technical Authority, COMDTINST 5402.3 (series)
 (f) Federal Financial Management Improvement Act (FFMIA) of 1996, 31 U.S.C. § 3512 (P.L. 104-208)
 (g) Sensitive Systems Policy, DHS Management Direction 4300A

- 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 establish, maintain, review, and improve internal controls through active involvement in assessments that both support assurances that the Coast Guard is accomplishing its intended objectives, and provide support information for the Commandant’s Assurance Statement.
- ACTION.** All Coast Guard unit commanders, commanding officers, officers-in-charge, deputy/assistant commandants, and chiefs of headquarters staff elements will comply with the provisions of this Commandant Instruction. Internet release is authorized.

DISTRIBUTION – SDL No.165

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A																										
B	*	X	X		X	X	X	X	X		X	X								X			X			X
C																										
D																										
E																										
F																										
G																										
H																										

NON-STANDARD DISTRIBUTION: Ba;(CG-092), (CG-094), (CG-1), (CG-12), (CG-13), PSC, CGA, (CG-2), (CG-4), (CG-5P), (CG-5R), (CG-7), (CG-8), (CG-9), DCO-I, FC, DOL, DCO, DCMS, LANT and PAC

3. DIRECTIVES AFFECTED. Coast Guard Internal Control Program Annual Statement of Assurance Requirements, COMDTINST 5700.10B, is cancelled.
4. BACKGROUND. Internal controls are essential to effective management of organizations. They comprise the plans, methods, and procedures used 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. In short, internal controls, which are synonymous with management controls, help government program managers achieve desired results through effective stewardship of public resources.
 - a. Internal controls should provide reasonable assurance that the following objectives are being achieved: effectiveness and efficiency of operations, reliability of financial and performance reporting, and compliance with applicable laws and regulations. A subset of these objectives is the safeguarding of assets. Internal controls should be designed to provide reasonable assurance regarding prevention or prompt detection of unauthorized acquisition, use, or disposition of an agency's assets.
 - b. Management has a fundamental responsibility to develop and maintain effective internal controls. The proper stewardship of Federal resources is an essential responsibility of agency managers and staff. Federal employees must ensure that Federal programs operate and Federal resources are used efficiently and effectively to achieve desired objectives. Programs must operate and resources must be used consistent with agency missions, in compliance with laws and regulations, and with potential high likelihood of preventing waste, fraud, and mismanagement.
 - c. Internal controls are considered a normal management responsibility, and all levels of management must involve themselves in assuring adequacy of internal controls.
 - d. Management is responsible for developing and maintaining an internal control system that integrates the five components of internal control as defined in reference (c): control environment, risk assessment, control activities, information and communications, and monitoring.
5. 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.
6. MAJOR CHANGES. Major changes include: the addition of many terms to the definitions section including amplified information on information technology general controls; the addition of a discussion section to frame the Coast Guard internal control program and annual cycle; and removal of specific deadlines for annual deliverables and assignment of Assessable Organizational Element designations.
7. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS.
 - a. The development of this directive and the general policies contained within it have been thoroughly reviewed by the originating office and are categorically excluded under current USCG categorical exclusion (CE-1) from further environmental analysis, in accordance with

Section 2.B.2. and Figure 2-1 of the National Environmental Policy Act Implementing Procedures and Policy for Considering Environmental Impacts, COMDTINST M16475.1 (series).

- b. This directive will not have any of the following: significant cumulative impacts on the human environment; substantial controversy or substantial change to existing environmental conditions; or inconsistencies with any Federal, State, or local laws or administrative determinations relating to the environment. All future specific actions resulting from the general policies in this Instruction must be individually evaluated for compliance with the National Environmental Policy Act (NEPA), Council on Environmental Policy NEPA regulations at 40 CFR Parts 1500-1508, DHS and Coast Guard NEPA policy, and compliance with all other environmental mandates. Environmental considerations were examined in the development of this directive and have been determined to be not applicable.
8. DISTRIBUTION. No paper distribution will be made of this Manual. An electronic version will be located on the following Commandant (CG-612) web sites. Internet: <http://www.uscg.mil/directives/>, and CGPortal: <https://cgportal2.uscg.mil/library/directives/SitePages/Home.aspx>.
9. RECORDS MANAGEMENT CONSIDERATIONS. This Instruction has been evaluated for potential records management impacts. The development of this Instruction has been thoroughly reviewed during the directives clearance process, and it has been determined there are no further records scheduling requirements in accordance with Federal Records Act, 44 U.S.C. 3101 et seq., National Archives and Records Administration requirements, and the Information and Life Cycle Management Manual, COMDTINST M5212.12 (series). This policy does not make any significant or substantial change to existing records management requirements.
10. DEFINITIONS.
 - a. Assessable Organizational Elements (AOEs): Designated at the discretion of management, AOEs are Coast Guard entities that manage processes with risks whose negative consequence would:
 - (1) Merit the attention of the Executive Office of the President and the relevant Congressional oversight committees;
 - (2) Violate statutory or regulatory requirements;
 - (3) Impair fulfillment of essential operations or missions; and/or
 - (4) Deprive the public of needed services.
 - b. Control Activities: Control activities are the actions management establishes through policies and procedures to achieve objectives and respond to risks in the internal control system, which includes the entity's information system.
 - c. Control Environment: The control environment is the foundation for an internal control system. It provides the discipline and structure, which affect the overall quality of internal control. It

influences how objectives are defined and how control activities are structured. The oversight body and management establish and maintain an environment throughout the entity that sets a positive attitude toward internal control.

- d. **Financial Management System:** A financial management system includes an agency's overall financial operation, reflecting the people, processes, and technology to capture, classify, summarize, and report data in a meaningful manner to support business decisions. It includes hardware, applications and system software, personnel, procedures, data, and reporting functions. The financial management system can be fully integrated with other management information systems (i.e., mixed systems) where transactions automatically flow into an accounting general ledger. The financial management system could also include manual processes to post transactions from other management systems into the accounting general ledger.
- e. **Financial System:** The financial system is an information system or set of applications that comprise the accounting portion of the financial management system that maintains all summary or detailed transactions resulting from budgetary and proprietary financial activity. The financial system encompasses processes and records that:
 - (1) Identify and record all valid transactions;
 - (2) Describe on a timely basis the transactions in sufficient detail to permit proper classification of transactions for financial reporting;
 - (3) Measure the value of transactions in a manner that permits recording their proper monetary value in the financial statements; and
 - (4) Determine the time period in which transactions occurred to permit recording of transactions in the proper accounting period.
- f. **Information and Communications:** Management uses quality information to support the internal control system. Effective information and communication are vital for an entity to achieve its objectives. Entity management needs access to relevant and reliable communication related to internal as well as external events.
- g. **Information Technology General Controls (ITGC):** General computer controls are one type of information processing controls included in the internal control component of control activities. These are the processes and procedures used to manage and control the DHS IT activities and computer environment. Reference (d) was created by GAO as the primary tool used by Federal Agencies to evaluate their IT controls. Chapter three of reference (d), *Evaluating and Testing General Controls*, describes six major categories of general controls that should be considered. Appendix A of reference (b), references these six domains:
 - (1) **Entity-wide Security Program Planning and Management (SP), FISCAM Section 3.1:** The processes and control activities used by an entity to provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the computer-related controls.

- (2) Access Control (AC), FISCAM Section 3.2: The processes and control activities in place to ensure that access to system resources and data is authenticated and authorized to meet the entity's financial, operational, and compliance objectives.
 - (3) Application Software Development and Change Control (CC), FISCAM Section 3.3:
 - (a) Application Software Development - The processes and control activities used by an entity to develop, configure, and implement new applications in order to meet the entity's financial, operational, and compliance objectives. This process is often referred to as the Software Development Lifecycle.
 - (b) Change Control - The processes and control activities used by an entity to ensure that modifications to programs continue to meet the entity's financial, operational, and compliance objectives.
 - (4) System Software (SS), FISCAM Section 3.4: The processes and control activities used by an entity to limit and monitor access to the powerful programs and sensitive files that (1) control the computer hardware and (2) secure applications supported by the system.
 - (5) Segregation of Duties (SD), FISCAM Section 3.5: The processes and control activities used by an entity to help ensure that one individual cannot control key aspects of computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to assets or records.
 - (6) Service Continuity (SC), FISCAM Section 3.6: The processes and control activities used by an entity to ensure that when unexpected events occur (e.g., disaster, service interruption, or loss of data), critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected.
- h. Internal Controls: Synonymous with management controls are a series of systematic measures, such as reviews, checks and balances, reconciliations, and methods and procedures that occur throughout an entity's operations on an ongoing basis to provide management with reasonable assurance that the goals and objectives management believes are important to the entity will be met.
- i. Mixed and feeder systems: A mixed system is a hybrid of financial and non-financial portions of the overall financial management system. Direct Access is an example of a feeder system used to support the Assistant Commandant for Human Resources (CG-1). Yard Time and Attendance and Surface Forces Logistics Center (SFLC) Industrial Operations Division Systems are examples of mixed systems. Any data transfer to the financial system from a mixed/feeder system must be:
- (1) Traceable to the transaction source;
 - (2) Controlled with sufficient automated and manual control activities to address information-processing objectives (completeness, accuracy, validity, and restricted access); and

- (3) In the data format of the financial system.
- j. **Materiality (Financial):** The omission or misstatement of an item in a financial report if, in light of surrounding circumstances, the magnitude of the item is such that it is probable that the judgment of a reasonable person relying upon the report would have been changed or influenced by the inclusion or correction of the item.
- k. **Materiality (General):** Material weaknesses for the purposes of assessing internal control are determined by management, whereas material weaknesses reported as part of a financial statement audit are determined by independent auditors. As the concept of non-financial materiality is more subjective, it is best defined in the context of reporting deficiencies in the design or performance of internal controls as follows:
 - (1) A control deficiency or combination of control deficiencies that in management's judgment represent significant deficiencies in the design or operation of internal control that could adversely affect the organization's ability to meet its internal control objectives is a reportable condition (internally tracked and monitored within the Coast Guard);
 - (2) A reportable condition (also known as a significant deficiency) that the agency head determines to be significant enough to be reported outside the agency will be considered a material weakness.
- l. **Monitoring:** Internal control is a dynamic process that has to be adapted continually to the risks and changes an entity faces. Monitoring of the internal control system is essential in helping internal control remain aligned with changing objectives, environment, laws, resources, and risks. Internal control monitoring assesses the quality of performance over time and promptly resolves the findings of audits and other reviews. Corrective actions are a necessary complement to control activities in order to achieve objectives.
- m. **Risk Assessment:** Having established an effective control environment, management assesses the risks facing the entity as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses. Management assesses the risks the entity faces from both external and internal sources.
- n. **Statement of Assurance (SOA) or Assurance Statement:** Reference (a) and DHS mandate that the Commandant annually prepare a statement as to whether the Coast Guard's systems of administrative and internal accounting controls comply with the requirements of FMFIA. If the systems do not comply, the report will include any material weaknesses in the Coast Guard's internal control systems and the plans and schedule for correcting any such weakness described. OMB issues guidance for evaluating these requirements in reference (b).
- o. **Test of Design:** A critical element in evaluation of an internal control, test of design reviews a control's planned performance against the objective the control is intended to address. Factors considered 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. Test of design starts with an assessment of risk and then tests a single sample's progress through the control process.

- p. Test of Effectiveness: An evaluation of the controls actual performance against the designed objective. Process samples are selected and tested to ensure the process is operating as it was intended.
11. DISCUSSION. Reference (e) directs the Assistant Commandant for Resources/Chief Financial Officer to establish and maintain a robust internal audit oversight over all three areas of internal control: operations, reporting, and compliance. This Commandant Instruction establishes policy for meeting internal control requirements to meet the requirements of reference (e). Further, this Commandant Instruction lays out the requirement that AOE's be responsible for providing assurance statements for effective and efficient business operations and compliance with laws and regulations within their respective areas. Coast Guard Internal Control Program Annual Statement of Assurance Requirements, COMDTNOTE 5200 is published annually, designating AOE's, and defining reporting requirements for the fiscal year.
- a. The objective of internal controls is to assist organizations in efficiently and effectively managing assets and their day to day operations. The purpose of standardizing internal control reporting within the Coast Guard is to improve management's critical decision support information.
- b. A top-down approach strategy sets the stage for successful implementation with the highest levels of leadership supporting the internal controls program.
- c. Managers must carefully consider the appropriate balance between controls and risk in their programs and operations. Too many controls can result in inefficient and ineffective processes; managers must ensure an appropriate balance between the strength of controls and the relative risk associated with particular programs and operations. The benefits of controls should outweigh the cost. For example, an aircrew's preflight checklist may delay response to a search and rescue event, but the benefit in flight safety is worth the cost of the operational delay. Managers should consider both qualitative and quantitative factors when analyzing costs against benefits.
- d. The Coast Guard performs its Management Control Plan (MCP) by using a standard four-phased approach. The four phases for development and execution of the MCP include:
- (1) Plan: Develop plans to evaluate control activities using a risk-based approach. This phase sets the tone for the entire MCP as key processes and control activities are identified that will be evaluated throughout the assessment cycle. Risk tolerance and materiality levels are determined and a top-down approach is applied to identify the significant high risk processes, objectives, and financial line items, and the associated entity and process level controls. These key control activities are documented on the risk assessment. Plans are then developed to assess control performance; controls addressing high risk processes and activities are planned for regular testing while low risk process controls can be evaluated less often.
 - (2) Assess: Perform internal control assessments that include tests of design, tests of operating effectiveness, self-assessments and verification and validation procedures. Based on the test of design plan developed during the planning phase, control activities

are assessed for the effectiveness of its control design. This assessment is achieved through interviews and walkthroughs with key process owners and documenting the processes in narratives, process flows, and work papers. A plan to test operating effectiveness is created based on controls activities that are determined to be designed effectively. 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. The Internal Control Working Group develops testing procedures and performs the tests with the support of the Office of Internal Controls, Commandant (CG-85). Commandant (CG-85) provides test sheet templates and verifies and summarizes test results. Control activities that do not appear to be designed or operating effectively are documented on workflow reports to identify control deficiencies and to develop corrective action plans with the key process owners.

- (3) Evaluate: Based on the control deficiencies identified during tests of design and tests of operating effectiveness, Commandant (CG-85) evaluates the magnitude and likelihood of misstatement and the impact to the organization's missions and objectives. Commandant (CG-85) prepares a summary of aggregated deficiencies to document and classify those deficiencies into the following categories: Control Deficiency, Reportable Condition, and Material Weakness. The preparation of the summary of aggregate deficiencies assists with logically evaluating the control deficiencies individually and in aggregate and identifying root causes and trends. The following steps outline the process to evaluating control deficiencies: (1) Identify the deficiencies, (2) Understand and assess each deficiency, (3) Assess likelihood of misstatement, (4) Assess potential magnitude of misstatement, (5) Identify compensating controls, (6) Determine classification of deficiencies, (7) Assess deficiencies in aggregation with others. Based on this evaluation, corrective action plans are developed to guide remediation efforts as management is accountable for taking corrective action.
 - (4) Report: Report results and impact as well as corrective action plans to Coast Guard leadership and external stakeholders such as DHS, Government Accountability Office (GAO), and Office of the Inspector General (OIG). The annual Coast Guard Statement of Assurance states management's conclusion on whether the internal controls are effective.
- e. Financial systems requirements are mandated by reference (f) and Appendix D of reference (b). Conformance also includes compliance with the Federal Information Security Management Act (FISMA) and OMB Circular No. A-130, Management of Federal Information Resources, as reportable conditions relate to financial management systems. For example, FISMA reporting of reportable conditions are to be reported as a lack of substantial compliance under FFMIA. Financial management systems include both financial and financially-related (or mixed) systems.
 - f. The Federal guidance to establish and assess information technology controls includes National Institute of Standards Technology (NIST) SP 800-53, Recommended Security Controls for Federal Information Systems, and OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems. DHS Management Directive (MD) 4300.1 establishes Departmental policy regarding IT Systems Security. Reference (g) provides detailed policy and procedural guidance.

- g. Attachment R of reference (g) contains the Compliance Framework for CFO Financial Systems, which identifies the 27 key information technology general controls that should be documented and tested annually for each CFO-Designated system to comply with OMB Circular A-123, Appendix A. The DHS Chief Information Officer (CIO) identified the 27 key ITGCs through an analysis of recurring control weaknesses in previous IT audit Notice of Finding and Recommendation (NFR) and these controls into the Attachment R. Reference (g) provides specific techniques and procedures for implementing the baseline security requirements that must be addressed in an IT security program.
- h. Internal control assessments will guide managers in identifying required remediation of key internal control deficiencies and should be viewed as a means of driving continuous improvement. The Office of Internal Controls, Commandant (CG-85) will be responsible for developing and communicating specific guidance consistent with this Instruction and relevant DHS directives. The objectives as established by reference (b) require reporting entities to focus on improving processes, controls, and maintaining supporting information that are most often used to manage an organization, all while continuing to work toward financial, operational, and compliance improvements that facilitate the achievement of organizational and authoritative objectives. Legislation enacted by Congress requires federal entities to provide more accountability for how resources are used and to provide assurance that the agency meets its objectives, and further requires that an audit be conducted over internal controls over financial reporting. Reference (a) requires that agency heads report annually on their controls. Reference (b) specifically requires agencies to implement a comprehensive management control program, provide statements of assurance that demonstrate the status of its internal controls, and that governance bodies be implemented to provide appropriate oversight of the management control program. To achieve these objectives, the Coast Guard implemented the below governance and oversight bodies:
- (1) The Executive Management Council - Internal Controls and Audit Readiness Board (EMC-ICARB) was established as the senior executive governance body to oversee the Coast Guard's financial audit activities and management control program;
 - (2) The Senior Assessment Team (SAT) was chartered as the execution arm of the EMC-ICARB by overseeing and coordinating key process remediation activities, mission action plan development and execution, and development of the Commandant's annual assurance statement.
 - (3) The Internal Control Working Group (ICWG) is led by the Office of Internal Controls and establishes working level relationships between Commandant (CG-85) staff and Coast Guard wide internal control coordinators for high risk and financially material processes.
 - (4) Coast Guard managers are responsible for establishing and maintaining internal control to achieve the objectives of effective and efficient operations, reliable reporting, and compliance with applicable laws and regulations. Managers will consistently apply the internal control standards to meet each of the internal control objectives and to assess internal control effectiveness.

12. POLICY. This Commandant Instruction establishes policy that the following objectives are being met:

- a. Resources are effectively and efficiently managed and applicable laws, regulations, and policies are complied with;
- b. Financial and all other resources are safeguarded from unauthorized use or disposition;
- c. Financial transactions are executed in accordance with authorizations;
- d. Records and reports are reliable (accurate and timely information is obtained, maintained, reported, and used for decision making);
- e. Financial systems conform to government-wide standards and appropriate internal controls are applied to all system inputs, processing and outputs; and
- f. Processes are managed to effectively and efficiently meet the objectives of operations, and program performance is measured and assessed.
- g. Management override of internal controls is not authorized. Controls need to be designed to account for unexpected inputs and extenuating circumstances that would require a deviation from routine business processes.

13. DUTIES & RESPONSIBILITIES.

- a. The Office of Internal Controls, Commandant (CG-85) is responsible for internal control oversight and reporting and will:
 - (1) Provide subject matter expertise, training, and assistance for complying with provisions of this Instruction;
 - (2) Be responsible for coordinating, documenting, and reporting on financial reporting internal controls, to include reference (b) documentation, walkthrough narratives and flow charts. Commandant (CG-85) will also be responsible for the risk assessment tools, test of design (TOD), and test of effectiveness (TOE) results, and summary of aggregated deficiencies (SAD);
 - (3) Provide AOE's with specific guidance and standard templates to fulfill reporting requirements over internal controls;
 - (4) Consolidate directorate level assurance statements in support of the Commandant's Assurance Statement;
 - (5) Report results as required by DHS; and
 - (6) Review and update this Commandant Instruction as necessary for any organizational and systemic changes applicable within the Coast Guard.

- b. AOE's will incorporate internal controls in their strategies, plans, guidance, and procedures that govern their programs, functions, and activities and will assess the operating effectiveness of those controls on an annual basis and will:
- (1) Be responsible for the data input to the mixed and feeder systems under their ownership and supervision, as well as the associated internal controls supporting those systems;
 - (2) Be responsible for the integrity of financial and non-financial data that managers use to manage program activity. An example of non-financial data is the information used to capture cutter and small boat activity in Abstract of Operations (AOPS);
 - (3) Be responsible for reporting on internal controls and compliance with applicable laws and regulations for their respective areas to Commandant (CG-85);
 - (4) Develop and implement a management control plan to include an annual risk assessment and an evaluation of the effectiveness of key controls;
 - (5) Produce and retain adequate supporting documentation to support internal control assurances;
 - (6) Provide an annual assurance statement based on their knowledge and understanding of their organization and relevant supporting documentation provided to them;
 - (7) Provide a copy of corrective action plan for any identified material weaknesses and reportable conditions;
 - (8) Provide a bridge letter to document any changes from the original statement of assurance through the end of the fiscal year as required. Supporting documentation is required for any changes identified in the bridge letter;
 - (9) Be responsible for the tenets of this Commandant Instruction and Coast Guard Internal Control Program Annual Statement of Assurance Requirements, COMDTNOTE 5200 through coordination and guidance from Commandant (CG-85); and
 - (10) Complete internal control assessment requirements as directed by Commandant (CG-85).
- c. Specific requirements in Appendix D of reference (b) and reference (f) dictate the following Commandant (CG-6) reporting requirements:
- (1) Provide an updated systems list to AOE's whenever there are changes to feeder and mixed systems;
 - (2) Monitor financial system non-conformances and plans for bringing systems into substantial compliance;
 - (3) Provide supporting documentation to justify reporting requirements for the annual Coast Guard Assurance Statement; and

- (4) Complete assessment and testing of information technology controls as required by reference (g).

14. FORMS/REPORTS. None.

15. REQUEST FOR CHANGES. Change requests should be submitted through the chain of command to Commandant (CG-85).

P. V. NEFFENGER /s/
Vice Admiral, U. S. Coast Guard
Vice Commandant