Chapter 2 – Standards of Conduct and Integrated Risk Management

Table of Contents

** Denotes hyperlink requiring CAC/NMCI access

References

(a) Code of Federal Regulations (CFR), Title 5 - Administrative Personnel

(b) DoD 5500.7-R, DoD Joint Ethics Regulations

(c) 41 U.S. Code, Public Contracts

(d) Public Law 104-106, National Defense Authorization Act for Fiscal Year 1996

(e) Federal Acquisition Regulations (FAR), Part 3 – Improper Business Practices and Personal Conflicts of Interest

(f) DoD Directive 5500.07, DoD Standards of Conduct

(g) SECNAVINST 5370.5C ,DON Hotline Program

(h) NAVSEAINST 5041.1B, DoD Hotline Program Policy and Procedures for NAVSEA

(i) DoD Instruction 7050.05, Coordination of Remedies for Fraud and Corruption Related to Procurement Activities

(j) SECNAVINST 5430.92C, Assignment of Responsibilities to Counteract Acquisition Fraud, Waste, and Related Improprieties within the Department of the Navy

(k) United States Code (U.S.C.), Title 10 - Armed Forces

(l) United States Code (U.S.C.), Title 31 - Money and Finance

(m) Federal Acquisition Regulation (FAR), Part 52 - Solicitation Provisions and Contract Clauses

(n) Federal Acquisition Regulation (FAR), Part 9 - Contractor Qualifications

(o) NAVSEAINST 5200.13D, Managers' Internal Control Program

(p) Government Performance and Results Act Modernization Act (GPRAMA)

(q) Federal Managers' Financial Integrity Act (FMFIA)

(r) OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control

(s) DON Integrated Risk Management Strategy

(t) GAO Standards for Internal Control in the Federal Government (GAO-14-704G)

(u) DON Integrated Risk Management Strategy

Figures

** Denotes hyperlink requiring CAC/NMCI access

Chapter 2 – Standards of Conduct and Integrated Risk Management

2.1 Introduction

Considering the significant power vested in Government officials, the public should expect the conduct of these officials to conform to the highest ethical standards. Congress has passed numerous ethics laws, and the Executive branch has published Government-wide regulations addressing the standards of ethical conduct expected of Government civilian and military personnel. (See 5 CFR 2635, reference (a), Standards of Ethical Conduct for Employees of the Executive Branch and DoD 5500.7-R, reference (b), DoD Joint Ethics Regulations). The importance of this topic is emphasized by the DoD requirement for acquisition personnel to receive periodic ethics training, which in the case of SUPSHIP personnel, is conducted by the command's office of legal counsel.

2.2 Procurement Integrity Act (PIA)

In the context of Federal procurements, Congress enacted the Office of Federal Procurement Policy Act, 41 U.S.C. 421, reference (c), which was amended by Public Law 104-106, reference (d), and is referred to as the Procurement Integrity Act (PIA). The PIA has been codified in 41 U.S.C. 2101-2107, reference (f), with detailed provisions identified in FAR 3.104, reference (e). Restrictions imposed by PIA include:

- improperly releasing or obtaining source selection information and contractor bid or proposal information (formerly referred to as "proprietary information")
- employment discussions between agency officials and contractors
- employment by contractors of former Government officials

2.2.1 Disclosing and Obtaining Procurement Information

The PIA prohibits specified personnel from disclosing certain procurement information, such as contractor bid or proposal information or source selection information. (See 41 U.S.C. 2102(3)). This prohibition applies to any person who is:

- a present or former officer or employee of the United States
- any person who is acting or has acted on behalf of the United States
- anyone who has advised the United States with respect to a Federal agency procurement and who, by virtue of his office, employment, or relationship, has access to bid, proposal, or source selection information

These personnel must not knowingly disclose such information before the award of the procurement to which the information relates. This applies only to procurements using competitive procedures.

** Denotes hyperlink requiring CAC/NMCI access

The law provides for criminal penalties, including fines and imprisonment for up to five years, if the disclosure was made in exchange for money or to give anyone a competitive advantage.

2.2.1.1 Obtaining Procurement Information

Unless otherwise provided by law, a person may not knowingly obtain contractor bid or proposal information, or source selection information, before award of the contract to which the information relates. Mere solicitation of procurement information does not violate the amended law. The same criminal penalties apply to knowingly obtaining procurement information.

2.2.2 Actions Required Regarding Offers of Non-Federal Employment

Per FAR 3.104-3(c), if an agency official who is participating personally and substantially in a competitive procurement in excess of $100,000 contacts, or is contacted by a bidder or offeror regarding non-Federal employment, they must report the contact in writing to their supervisor or the designated ethics official and either reject the possibility of non-Federal employment or disqualify themself from participating in the procurement. Participating personally and substantially in a Federal procurement is defined in FAR 3.104-1. Civil or administrative penalties can be imposed for violations of this prohibition.

A written notice of disqualification goes to the Head of the Contracting Activity (HCA), or their designee, with concurrent copies to the immediate supervisor, the contracting officer, the Source Selection Authority (SSA), and the local legal office. Copies of these disqualifications must be kept for two years.

2.2.3 Post-Government Employment Restrictions

41 U.S.C. 2104 provides for a one-year prohibition on receipt of compensation from certain contractors if a former official served in certain capacities or made certain decisions on behalf of the Government. Under the law, a former agency official must not accept compensation from a contractor within one year of performing any of the following actions:

- Serving as the Procuring Contracting Officer (PCO), SSA, member of the Source Selection Evaluation Board (SSEB), or the chief of a financial or technical evaluation team. This applies for a procurement in which the contractor was selected for award of a contract in excess of $10 million.

- Serving as the program manager, deputy program manager, or Administrative Contracting Officer (ACO) for a contract in excess of $10 million awarded to the contractor.

- Personally making a decision to:

    - award a contract, subcontract, modification of a contract or subcontract, or a task or delivery order in excess of $10 million to the contractor

    - establish overhead or other rates applicable to a contract or contracts for the contractor that are valued in excess of $10 million

** Denotes hyperlink requiring CAC/NMCI access

- approve issuance to the contractor of a contract payment or payments in excess of $10 million

- pay or settle a claim with the contractor in excess of $10 million

Civil or administrative penalties can be imposed on both the former official and the contractor for violations of this prohibition.

A former official is not prohibited from accepting compensation from any division or affiliate of a contractor that does not produce the same or similar products or services as the entity of the contractor that is responsible for the contract. This restriction applies to sole source and competitive contracts in excess of $10 million (includes value of contract at award and all options).

The Designated Agency Ethics Official (DAEO), or their designee, will give a safe harbor (i.e., ethics advisory opinion) to any employee or former employee who wishes to know whether the individual can accept compensation from a particular contractor subsequent to their separation from the Government.

In addition to the post-employment restrictions mentioned above, a criminal statute in 5 CFR 2641, Post-Employment Conflict of Interest Restrictions, contains several post-employment restrictions that apply to certain former employees, including a basic prohibition that:

"No former employee shall knowingly, with the intent to influence, make any communication to or appearance before an employee of the United States on behalf of any other person in connection with a particular matter involving a specific party or parties in which he participated personally and substantially as an employee and in which the United States is a party or has a direct and substantial interest." [5 CFR 2641.201]

Employees should consult their ethics advisor for advice on specific post-employment restrictions that may apply to them.

2.2.4 Determining Violations or Possible Violations

If the contracting officer receives or obtains information of a violation or possible violation of the law, that officer is required to determine whether it has an impact on the pending award or source selection. If the contracting officer determines that it does impact the procurement, they must forward this information to the HCA or their designee. The HCA may request information from appropriate parties and will review all relevant information. If the HCA determines that the Act has been violated, the HCA may direct the contracting officer to cancel the procurement, disqualify an offeror, or take other appropriate action.

2.3 Measures to Minimize Improper Conduct

SUPSHIP personnel should be familiar with the requirements of FAR 3.104, DoDD 5500.07 (Standards of Conduct), reference (f), and the DoD Joint Ethics Regulation. They must understand that violation of these regulations may result in disciplinary action and that violations of ethics statutes may result in civil and/or criminal penalties.

** Denotes hyperlink requiring CAC/NMCI access

SUPSHIP should analyze and identify operations with potential for misconduct. When warranted, SUPSHIP should develop and execute a plan to minimize that potential misconduct. The following should be considered in formulating such a plan:

- increase surveillance by supervisors of Government personnel at remote contractors' sites through unscheduled inspections of specific operations
- reduce tour length of Government personnel at remote sites
- rotate Government personnel among contractor sites
- require that preparation of a specification and inspection or acceptance of work under that specification be performed by different individuals
- audit work authorized on-site for actual completion
- audit accepted work for conformance to specifications
- audit Government Property Administrator's decisions on scrap, repairables, and mandatory returnables
- audit scrap materials sold to contractors by Government property administrators to ensure that materials are scrap
- be alert for signs of affluence not commensurate with the economic status of Government employees
- ensure all SUPSHIP personnel understand the command requirement for absolute adherence to the Standards of Conduct
- be observant for possible falsification of inspection records

2.4 Hotline Policies and Procedures for NAVSEA Shore Activities

SECNAVINST 5370.5C, DON Hotline Program, reference (g), discusses the requirement for military and civilian personnel to report suspected fraud, waste, abuse, mismanagement, and ethics violations to appropriate authorities. The chain of command is the preferred means of reporting because it reinforces accountability and allows matters to be addressed at the lowest level. The DoD/DON Hotline Programs provide confidential and reliable alternatives when a complainant fears reprisal or believes the chain of command has been unresponsive. NAVSEAINST 5041.1B**, NAVSEA Hotline Program, reference (h), encourages employees of NAVSEA employees to use the chain of command or to use the local, NAVSEA, Navy, or DoD Hotlines to report fraud or related improprieties.

A Hotline may be established at the discretion of the commanding officer. The instruction ensures that Hotline referrals are forwarded to NAVSEA, that complete records and controls are established and maintained, and that examiners are independent, impartial, and free of actual or perceived

** Denotes hyperlink requiring CAC/NMCI access

influence. The instruction gives procedures on publicizing information about Hotline programs and contacting appropriate authorities to respond to fraud or related improprieties.

2.5 Fraud, Waste, and Other Abuse

This section discusses coordination of fraud prevention, indicators of fraud, and actions against fraud.

2.5.1 Coordination for Fraud Prevention

DoD officials are responsible for the integrity of DoD contracts and must be prepared to take immediate action to protect Government integrity and interests when required. Although criminal cases often take years to complete, the DoD can take contractual and administrative actions on less evidence than needed for a criminal conviction. A coordinated approach to criminal, civil, contractual, and administrative actions permits the Government to expedite criminal proceedings. Early action and coordination are essential to ensure that no action taken will adversely affect the Government's ability to pursue any other available action.

The Secretary of Defense (SECDEF) issued DoDI 7050.05, reference (i), to establish centralized points of coordination. This directive requires that the cognizant criminal investigative organizations inform the centralized points of coordination each time a significant fraud or corruption investigation in procurement or related activities is opened. Through this process, the Government can use a variety of remedies in a more efficient and effective manner. In 2007, SECNAV established the Acquisition Integrity Office (AIO) to manage acquisition fraud matters within DON. Per SECNAVINST 5430.92C, reference (j), AIO acts as the centralized organization within DON to monitor and ensure the coordination of all criminal, civil, administrative, and contractual remedies for all cases, including investigations for fraud, waste, and related improprieties related to DON acquisition activities. As the centralized organization for acquisition fraud matters, AIO is the single point of contact for all acquisition fraud matters. AIO partners with NCIS and the Naval Audit Service (NAS) to provide investigative support on acquisition fraud cases.

2.5.2 Indicators of Defective Pricing Fraud

Auditors assess pricing situations to determine if the circumstances surrounding any defective pricing is an indicator of potential fraud. The auditor is responsible for finding and reporting indicators, not proving fraud. The Truth-in-Negotiations Act (TINA), codified in 10 U.S.C. 2306a, reference (k), and 41 U.S.C. Ch. 35, gives the Government the right to adjust the contract price when the price is based on inaccurate, incomplete, or out-of-date cost or pricing data. Defective pricing occurs when more current, complete, and accurate data exist, but are not provided to the negotiator.

The Defense Contract Audit Agency (DCAA) is responsible for performing reviews of selected contracts and subcontracts. The agency issues a defective pricing report when the auditor finds that the contract price was increased because the contractor did not follow the Truth-in-Negotiations Act. In the past, auditors concentrated on finding defective pricing and not assessing the reason for defective pricing and indications of fraud. The DCAA issued guidance by providing a list of indicators for assessing whether the situation is a sign of possible fraud that should be referred for

** Denotes hyperlink requiring CAC/NMCI access

investigation. The following are possible indicators of defective pricing fraud that demonstrate the need for further investigation:

- using a vendor other than the proposed vendor
- intentional failure to update cost or pricing data
- selective disclosure
- changed dates
- lost records
- lack of support for proposal
- change in make-versus-buy decisions
- reporting a production break and increased cost when no actual break occurs
- combining items
- intentionally eliminating support to increase the proposal prices
- including inflated rates in the proposal, for example, for insurance or workers' compensation
- intentionally duplicating costs by proposing them as both direct and indirect
- indication of other fraudulent activities which would include material substitution, used or new, and certifying replacement of parts versus repair
- proposing obsolete items that are not needed
- continually failing to provide requested data
- not disclosing an excess material inventory that can be used in later contracts
- refusing to provide data which is requested for elements of proposed costs
- not disclosing actual data from completed work for follow-on contracts
- knowingly using an inter-company division to perform part of the contract but proposing purchase or vice versa
- ignoring established estimating practices
- suppressing studies that do not support the proposed costs
- commingling work orders to hide productivity improvements
- requesting an economic price adjustment clause when the material is already purchased
- submitting fictitious documents
- withholding information on batch purchases
- failing to disclose internal documents on vendor discounts
- failure of prime contractor to pay subcontractor

** Denotes hyperlink requiring CAC/NMCI access

2.5.3 Actions Against Fraudulent Activities

The Government has the right to insist on certain standards of responsibility and business integrity from its contractors and to take a variety of actions against contractors who engage in fraudulent activities. These actions described below are taken in conjunction with, after, or instead of criminal prosecution.

The Civil False Claims Act, 31 U.S.C. 3729, reference (l), can make a contractor liable for submission of a false claim to the Government and allows the Government to recover damages and penalties for false claims. The Government must suffer monetary damages to recover damages and must prove by a preponderance of evidence that the contractor knowingly submitted a false claim.

The Program Fraud Civil Remedies Act, 31 U.S.C. 3801, allows Federal agencies to impose administrative penalties for certain false claims and statements.

The Contract Disputes Act, 41 U.S.C. 7101-7109, makes a contractor liable for the amount of any unsupported part of a claim plus the costs of reviewing the claim if it is determined that it is a result of misrepresentation of fact or fraud.

The courts can order the forfeiture of the entire amount of a claim in which it judges the proof is based on contractor fraud or attempted fraud. A contractor risks losing the entire claim even if the claim is only partially based on fraud.

The contracting office has the right to terminate a contract for default because of a contractor's failure to perform. The Government also has the right to terminate a contract for default for other improper conduct, including violation of the Anti-Gratuities Clause (FAR 52.203-3), reference (m) and 41 U.S.C. 51- 58, the Anti-Kickback Act of 1986, which prohibits gifts by a subcontractor as inducement for award of the contract.

Rescission is a common law remedy in contracts which allows both parties to return to their position before the contract. This remedy may be used when fraud or corruption occurs in obtaining or awarding the contract. The Government may administratively rescind a contract when there has been a final conviction for bribery, gratuities, or conflicts of interest.

Per 41 U.S.C. 605, contracting officials do not have the authority to pay claims where there is reasonable suspicion of fraud. Contracting officials should not take further action without coordination with the Department of Justice. The provisions of FAR 9.1, reference (n), state that contracts may only be awarded to responsible contractors. Contractors must affirmatively demonstrate their responsibility, including a satisfactory record of integrity and business ethics.

Per FAR 9.4, contractors may be prohibited from doing business with the Government for the commission of fraud. Suspension is an interim measure; a contractor may be suspended for up to 18 months while the investigation is underway. Debarment is a final determination of a contractor's non-responsibility and may be effective for up to three years. A contracting officer can recommend the debarment of companies and individuals and can impute, in recommending its debarment, the conduct of certain key individuals in that company. Contracting officials must forward reports of improper contractor activity to the suspension and debarment authority at the earliest opportunity to make suspension or debarment effective.

** Denotes hyperlink requiring CAC/NMCI access

Under FAR 31.205-47, contractors who are found to have engaged in fraud on cost-type contracts are not entitled to recover legal and administrative costs incurred in unsuccessfully defending against Government action.

10 USC 2408, Prohibition on Persons Convicted of Defense Contract-Related Felonies and Related Criminal Penalty on Defense Contractors, bars an individual convicted of fraud or any other felony arising from a contract with the DoD from working in management or a supervisory capacity on any defense contract.

Under 10 USC 2324, a contractual penalty can be assessed when a contractor submits a claim for a direct or indirect cost when such a cost is specifically ruled unallowable by either statute or regulation. The statute also authorizes a penalty for the knowing submission of defective cost or pricing data.

2.5.4 Government Personnel

The Government has a variety of remedial actions to take against employees who collude with contractors in fraudulent conduct, including termination, revocation of a contracting officer's warrant, recoupment of lost funds, and administrative penalties for conflicts of interest.

2.6 Managers' Internal Control Program (MICP)

The Navy is incorporating the Managers' Internal Control Program (MICP) into the broader-scope Integrated Risk Management (IRM) Strategy. IRM guidance is forthcoming with the imminent release of the DON IRM Guidebook, DON IRM Implementation instructions, and SECNAVINST 5200.35H. When those documents are released, this section and the SUPSHIP MICP Manual, appendix 2-B, will be updated accordingly.

NAVSEAINST 5200.13D**, Managers' Internal Control Program, reference (o), states NAVSEA's policy on internal controls and requires that all commands establish MICPs to support commanders and managers in meeting the requirements of OMB Circular A-123 (21 Dec 2004). In 2016, however, OMB published the revised OMB Circular A-123 (15 Jul 2016), reference (p), to modernize existing efforts by requiring agencies to implement an Enterprise Risk Management (ERM) capability coordinated with the strategic planning and strategic review process established by the Government Performance and Results Act Modernization Act (GPRAMA), reference (q), and the internal controls process processes required by the Federal Managers' Financial Integrity Act (FMFIA), reference (r), and the Government Accountability Office (GAO) Standards for Internal Control in the Federal Government (GAO-14-704G), reference (s).

OMB Circular A-123, reference (t), describes ERM and Internal Control as components of a governance framework. ERM, as a discipline, deals with identifying, assessing, and managing risks. Through adequate risk management, agencies can concentrate efforts towards key points of failure and reduce or eliminate the potential for disruptive events. Internal control is a process effected by an organization's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an organization will be achieved.

** Denotes hyperlink requiring CAC/NMCI access

Operating under the current NAVSEAINST 5200.13D** guidance, MICP is a tool to evaluate and report on the effectiveness of internal controls throughout an organization and to identify necessary corrective actions to remedy deficiencies. The establishment and verification of internal control effectiveness is essential for leadership to establish reasonable assurance that operational risks are mitigated, and internal control deficiencies are promptly identified for corrective action.

The SUPSHIP Managers' Internal Control Program Manual, Appendix B, mandates establishment of an MICP at each SUPSHIP to support the Supervisor and managers in assessing operational risk, implementing and validating the effectiveness of internal controls, implementing corrective actions as internal control deficiencies are identified, and reporting on the effectiveness of internal controls. It also describes the minimum requirements for MICP execution for consistent application across SUPSHIP offices and to ensure that the Supervisors receive quality and consistent MICP products.

2.7 Integrated Risk Management (IRM) (formerly MICP)

In 2020, SECNAV issued the DON Integrated Risk Management Strategy, reference (u). The strategy outlines the framework necessary for DON to more effectively manage strategic risk in accordance with OMB Circular A-123. ERM is the Navy-wide approach to addressing the full spectrum of external and internal risks by understanding the combined impact of risks as an interrelated portfolio. IRM is DON's approach to integrating its ERM strategy and outlines key requirements of ERM and Internal Controls Over Reporting (ICOR). ICOR is defined in the GAO Standards for Internal Control in the Federal Government (GAO-14-704G) as a process for providing reasonable assurance that the objectives of an organization are achieved.

IRM is intended to identify, prioritize, and focus the management of key enterprise risks that could impede achievement of strategic objectives. It emphasizes the importance of focusing on the DON's most critical risks, assessing those risks holistically, and increasing the quality of data and reports by performing an ICOR assessment.

IRM improves DON's strategic risk management capability by:

- Strengthening governance to enable senior leaders to effectively drive "Tone at the Top" (importance of director/commander support of the overall control environment and organizational culture)
- Integrating ERM and ICOR programs to facilitate a top-down, bottom-up approach to risk management driven by quality data
- Evolving the existing DON A-123 MICP to ICOR
- Implementing an enterprise, Governance, Risk, and Compliance (eGRC) technology platform to integrate and automate all risk management activities

2.7.1 MICP Transition to IRM

IRM implementation is dependent upon integrating DON's ERM and ICOR programs, enabling the efficient flow of risk management and internal control information through a unified technology platform, and the oversight provided by governance bodies that have timely access to reliable information.

** Denotes hyperlink requiring CAC/NMCI access

The DON IRM Program Office will implement the DON IRM strategy beginning in FY22 and will work continually with stakeholders to mature IRM capabilities moving forward.

As the IRM Program matures, risk management activities will be prioritized in accordance with the DON Risk Profile, commander's priorities, and priorities established by DON's end-to-end process owners. Outcomes from the ongoing DON full financial statement audit and feedback from internal and external oversight bodies such as the GAO, DoD Inspector General, and Independent Public Accountant will continue to inform DON leadership of risks that must be prioritized at the enterprise level and subsequently mitigated and/or monitored.

The figure below, taken from the DON Integrated Risk Management Strategy, reference (u), provides an overview of the transition from MICP to IRM. Note that Appendix A of OMB Circular A-123 went through a major revision that expanded the focus of internal control reporting to all reports (financial and non-financial). As a result, the current Internal Controls Over Financial Reporting (ICOFR), Internal Controls Over Financial Systems (ICOFS), and Internal Controls Over Operations (ICO), are being consolidated into ICOR.

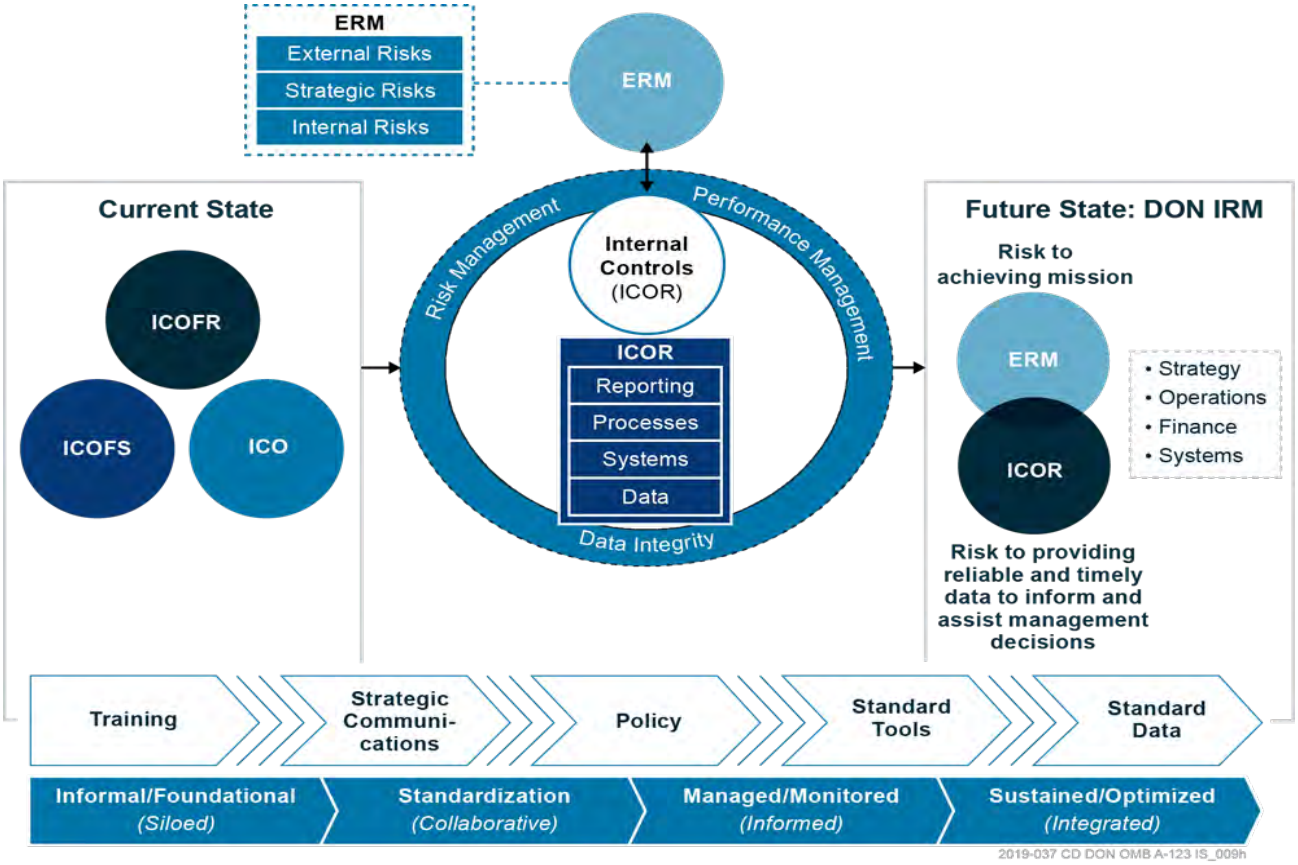


Figure 2-1. Broadened OMB Circular A-123, Appendix A (2018)

While it is anticipated that SUPSHIPs will continue to maintain the essential elements of an MICP under ICOR, the nature and degree of command-level involvement in ERM has yet to be determined. SEA 04Z will be collaborating with the SUPSHIPs to develop appropriate community guidance as additional higher-level direction is published.

** Denotes hyperlink requiring CAC/NMCI access

Appendix 2-A: Acronyms

ACO	Administrative Contracting Officer
AIO	Acquisition Integrity Office
AMCR	Alternative Management Control Review
AU	Assessable Unit
CCB	Configuration Control Board
CFR	Code of Federal Regulations
DAEO	Designated Agency Ethics Official
DCAA	Defense Contract Audit Agency
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoN	Department of the Navy
eGRC	Enterprise Governance, Risk, and Compliance
ERM	Enterprise Risk Management
FAR	Federal Acquisition Regulations
HCA	Head of the Contracting Activity
ICO	Internal Controls Over Operations
ICOR	Internal Controls Over Reporting
ICOFS	Internal Controls Over Financial Systems
ICOR	Internal Control Over Reporting
IR	Item to be Revisited
IRM	Integrated Risk Management

MCR	Management Control Review
MICP	Managers' Internal Control Program
MW	Material Weakness
NAS	Naval Audit Service
NAVSEA	Naval Sea Systems Command
NAVSEAINST	Naval Sea Systems Command Instruction
NCIS	Naval Criminal Investigative Service
OMB	Office of Management and Budget
PCO	Procuring Contracting Officer
PIA	Procurement Integrity Act
PL	Public Law
RC	Reportable Condition
SOA	Statement of Assurance
SECDEF	Secretary of Defense
SECNAVINST	Secretary of Navy Instruction
SSA	Source Selection Authority
SSEB	Source Selection Evaluation Board
TINA	Truth in Negotiations Act
USC	United States Code

Appendix 2-B: SUPSHIP Managers' Internal Control Program (MICP) Manual

The Navy is transitioning from the Managers' Internal Control Program (MICP) to the Integrated Risk Management (IRM) Strategy. This manual will be updated after the release of the DON IRM Guidebook, DON IRM Implementation instructions, and SECNAVINST 5200.35H.

Supervisor of Shipbuilding Managers' Internal Control Program (MICP) Manual

2 April 2017

Supervisor of Shipbuilding

Managers' Internal Control Program (MICP) Manual

Table of Contents

References

(a) OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control

(b) NAVSEA 5200.13D, Management Control Program

(c) GAO-14-704G, Standards for Internal Control in the Federal Government

(d) DoDI 5010.40, Managers' Internal Control Program Procedures

(e) SECNAV 5200.35F, DoN Managers' Internal Control Program

(f) SECNAV M-5200.35, DoN Managers' Internal Control Manual

Tables

1. Purpose

This operating manual establishes the mandatory policies, procedures, and responsibilities for the implementation and administration of the Managers' Internal Control Program (MICP).

2. Scope

This manual is effective immediately and is applicable to all Supervisors of Shipbuilding, Conversion, and Repair, USN (SUPSHIPs). All locally issued SUPSHIP instructions establishing an MICP must reference this manual as a mandatory-use document.

3. Background

a. OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, reference (a), states:

> *"Federal leaders and managers are responsible for establishing goals and objectives around operating environments, ensuring compliance with relevant laws and regulations, and managing both expected and unexpected or unanticipated events. They are responsible for implementing management practices that identify, assess, respond, and report on risks. Risk management practices must be forward-looking and designed to help leaders make better decisions, alleviate threats and to identify previously unknown opportunities to improve the efficiency and effectiveness of Government operations. Management is also responsible for establishing and maintaining internal controls to achieve specific internal control objectives related to operations, reporting, and compliance."*

b. Per NAVSEA 5200.13D**, Managers' Internal Control Program, reference (b), commanders and managers are responsible for ensuring that resources under their cognizance are used efficiently and effectively, and that programs and operations are discharged with integrity and in compliance with applicable laws and regulations. Implementation of the MICP establishes a system of internal controls which encompasses all programs and functions within NAVSEA, not just the comptroller functions of budgeting, recording, and accounting for revenues and expenditures. The MICP should not be a separate system in an activity; it should be an integral part of the systems used to operate the programs and functions performed by the activity. The General Accounting Office (GAO) standards for internal control in the Federal Government state that effective management controls:

1) Establish and maintain an environment throughout the organization that sets a positive and supportive attitude toward internal control and conscientious management;

2) Provide an assessment of the risks from both external and internal sources;

3) Help ensure that management's directives are carried out;

** Denotes hyperlink requiring CAC/NMCI access

4) Record and communicate reliable information to those who need it, in a format that is relevant and timely; and

5) Assess the quality of performance over time and ensure that the findings of audits and other reviews are promptly resolved per GAO-14-704G, Standards for Internal Control in the Federal Government, reference (c).

Additional MICP guidance is provided by:

- DoDI 5010.40, Managers' Internal Control Program Procedures, reference (d)
- SECNAV 5200.35F, DoN Managers' Internal Control Program, reference (e)
- SECNAV M-5200.35, DoN Managers' Internal Control Manual, reference (f).

4. MICP Implementation

a. Each SUPSHIP shall implement a system of internal controls to provide reasonable assurance that the following objectives are met:

1) Effective and efficient operations

2) Reliable financial reporting

3) Compliance with applicable laws and regulations

b. Each SUPSHIP shall implement an MICP to support commanders and managers in assessing operational risk, identifying internal controls necessary to mitigate these risks, validating the implementation and effectiveness of these internal controls, implementing corrective actions as internal control deficiencies are found, and reporting on the effectiveness of internal controls.

c. Each SUPSHIP MICP shall consist of the following key components:

1) MICP Plan

2) Inventory of Assessable Units

3) Risk Assessment Process

4) Internal Control Assessment Documentation

5) Annual Statement of Assurance (SOA)

5. MICP Plan

a. The MICP Plan is an executive summary of a command's MICP. The plan captures the organization's approach to implementing an effective internal control program. As required by SECNAV M-5200.35, DoN Managers' Internal Control Manual, the MICP plan shall be updated annually and must identify the following key elements:

1) The organization's senior official overseeing the MICP, the MIC coordinator and the alternate MIC coordinator

2) An overview of the MICP as related to the GAO standards for internal control
3) A description of risk assessment methodology
4) A description of monitoring/internal control assessment methodology
5) A description of how to develop and track corrective action plans
6) MIC training efforts
7) The date the plan was last updated

b. An MICP Plan development guide is provided in Example 7 of SECNAV M-5200.35. The guide outlines the key information requirements for each section to provide assistance in developing a robust plan. This format shall be used by each SUPSHIP MIC Program Coordinator to create the organization's plan, which must be updated at least annually.

6. Inventory of Assessable Units

a. NAVSEAINST 5200.13D** requires that each MICP Coordinator establish and maintain an inventory of assessable units (AUs) for the activity's key financial and operational processes, and defines an assessable unit as "Any organizational, functional, programmatic, or other applicable subdivision capable of being evaluated by management control assessment procedures. An assessable unit should be a subdivision of an organization that ensures a reasonable span of management control to allow for adequate analysis." SECNAV M-5200.35 states that "An assessable unit must have clear limits or boundaries and be identifiable to a specific responsible manager. Further, it must be small enough to provide reasonable assurance of adequate management controls but large enough that any detected material weakness has the potential to impact the mission of the organization. Assessable units must constitute the entire organization. This means that every part of the organization must be represented by one of the assessable units in the organization's inventory of assessable units."

b. SUPSHIP MICP Coordinators will collectively develop and maintain an AU Inventory consisting of AU's common to all SUPSHIPs. Each SUPSHIP MICP must include and account for these common AU's and their associated internal controls in their command's MICP. SUPSHIP MICP Coordinators must also maintain an inventory of additional AU's that are unique to one or more SUPSHIPs (e.g., SUBSAFE Program). Enclosure (1) provides a sample AU Inventory that may be utilized by SUPSHIP MIC Coordinators to document the command AU inventory.

c. AUs must properly reflect the organization and be updated as necessary to reflect changes within the organization and/or its functional managers. At a minimum, the SUPSHIP common and unique AU inventory must be reviewed annually to ensure its accuracy.

d. The SUPSHIP AU Inventory will contain, at a minimum, the following data:

- AU name

** Denotes hyperlink requiring CAC/NMCI access

- Identification of SUPSHIP common AUs
- AU description/definition
- Name of the AU manager (AUM)/assessor

e. The above data fields should be populated through ongoing collaboration between MIC Program Coordinators and AU Managers. At least annually, MICP Coordinators and AU Managers will review and update these data fields, including validating that the existing AU Inventory accurately reflects the command's current workload and responsibilities.

7. Risk Assessment Process

a. The MICP Risk Assessment process is intended to identify the likelihood and consequence of a process control failure that may impact the organization in meeting its objectives. Designated AU Managers will complete AU Risk Assessments in accordance with paragraph 7(c) and 7(d) below. When assessing the likelihood of process control failures, AU Managers should take into account the adequacy and accuracy of AU process documentation, personnel and budgetary resources available to execute these processes, the extent to which these processes are reviewed, and the adequacy of corrective action procedures for identified deficiencies. When assessing the consequence of process control failures, AU Managers should consider the potential visibility of a control failure, resulting work stoppage issues, impact to personnel or equipment safety, disciplinary actions, and the extent to which the impact of the control failure will be known or contained.

b. When completing AU risk assessments, AU Managers should also consider uncorrected findings from audits, inspections, or internal reviews and their potential effect or impact on the ability of the command to meet its mission.

c. AU Risk Assessments should be performed at least annually. AU Risk Assessments should also be completed in the following circumstances:

- When a new AU Manager is assigned
- When a new AU is added to the command AU inventory

d. All SUPSHIP AU Managers will utilize the template in enclosure (2), the Assessable Unit Risk Assessment Form, to perform risk assessments. AU Managers or designated Subject Matter Experts (SMEs) should complete the Risk Assessment Form. Risk Assessments performed by someone other than the designated AU Manager must be approved by the designated AU Manager.

e. MICP Coordinators will utilize AU Risk Assessment results to prioritize the MICP effort, including:

- Coordinating identification of AUs that are at high risk for fraud, waste, abuse, and/or mismanagement

- Identifying AU's where management control improvement is required to reduce the likelihood of a process control failure

f. SECNAV M-5200.35 defines three types of risk:

1) Inherent Risk: the original susceptibility to a potential hazard or material misstatement assuming there are no related specific control activities

2) Control Risk: the risk that a hazard or misstatement will not be prevented or detected by the internal control

3) Combined Risk: the likelihood that a hazard or material misstatement would occur and not be prevented or detected on a timely basis by the organization's internal controls

g. Using the AU Risk Assessment Form, enclosure (2), AU Managers, in collaboration with MICP Coordinators, will identify the level of inherent risk and control risk associated with each identified risk and management control within their applicable AU's. The form's Combined Risk Matrix will then assign a combined risk level for each risk based on a green (low risk), yellow (moderate risk), red (high risk) color scale. Table 1 provides a narrative description of each of these risk levels. Although the AU Risk Assessment Form and Table 1 may provide useful guidance, assessing risk and determining the adequacy of internal controls is ultimately a decision made by the AU Manager and MICP Coordinator based on management judgment and subject matter expertise.

Table 1 – Levels of Inherent, Control, and Combined Risk

Risk	Low	Moderate	High
Inherent	AU Manager believes the potential risk does not have severe consequences and is unlikely to occur.	AU Manager believes the potential risk has severe consequences or is likely to occur.	AU Manager believes the potential risk has severe consequences and is likely to occur.
Control	AU Manager believes the controls in place will prevent or detect a process control failure.	AU Manager believes controls in place will more likely than not prevent or detect a process control failure.	AU Manager believes the controls in place are unlikely to prevent or detect a process control failure.
Combined	AU Manager believes likelihood of hazard or process failure does not pose significant threat to mission, resources, or image,	AU Manager believes potential for a hazard or process failure indicates greater attention needed monitoring/improving controls.	AU Manager believes likelihood of significant hazard or process failure suggests implementation of effective controls are imperative.

8. Internal Control Assessment Documentation

a. In accordance with SECNAV M-5200.35, once internal controls are in place, management shall actively monitor those controls to ensure that they are functioning correctly and effectively mitigating the associated risk. At the MICP Coordinator's discretion, SUPSHIPs will document assessments of an AU's internal controls on the either the Excel version of the AU Internal Control Assessment Summary form, enclosure (3A), or the PDF version, enclosure (3B).

b. Control assessment documentation can include either Management Control Review (MCR) results or Alternative Management Control Review (AMCR) results. An MCR is a documented evaluation on the effectiveness of an internal control in meeting the control objective.

c. MCRs conducted at SUPSHIPs will be documented using the template provided in enclosure (4) and will provide the following information:

1. Assessable Unit
2. Name of individual conducting the evaluation
3. Identify control being assessed and associated risk(s)
4. Identify Control Type
5. Method of Testing Key Controls
6. Assessment Results
7. Internal control deficiencies/weaknesses detected, if any
8. Corrective actions
9. Certification and signature

d. AMCR is a process developed for other organizational purposes which determines whether or not a management control is operating effectively. Alternative Management Control Reviews may include, but are not limited to, the following:

- SUPSHIP Command Evaluation and Review Office Internal Reviews
- Results of audits performed by external agencies including Government Accountability Office, DoD Inspector General, and Naval Audit Service
- NAVSEA Command Compliance Inspections
- Command Investigations
- Internal audits or self-assessments

- Existing organizational evaluations

e. Every assessable unit should be subject to at least one MCR annually, unless all identified management controls are reviewed as a function of an AMCR. An MCR performed by an AU Manager does not need to include all controls each year. The scope of the MCR is based on management's judgment, and should focus first on areas where control risk is identified as medium or high.

In accordance with NAVSEA 5200.13D, the AU Manager should provide flow charts or process maps as part of the internal control evaluation process. It is not necessary to provide detailed charts of all processes included in the AU. The charts or maps are solely intended to provide a simple depiction of how the control will mitigate the applicable risk or risks. See SECNAV M-5200.35 (Example 8, page 29) for a sample process flowchart.

All MCRs conducted by the assigned AU Manager, the MICP Coordinator, or an external agency, will be identified as a management control validation effort in the Command's AU control assessment. To ensure that all internal control validation efforts are properly accounted for, and to avoid any potential duplicity of control validation efforts, all AMCR documentation, including audit reports and self-assessment results, should be provided by the cognizant AU Manager to the MICP Coordinator as it becomes available.

f. All identified management controls will be rated as having a low, moderate, or high control risk. If the results of an AMCR or MCR find the management control to be ineffective, the control should be reclassified as having a high control risk. A corrective action plan, found in enclosure (4), should be developed for any controls that are classified as having a high control risk.

g. All Management Control Reviews that identify internal control deficiencies require corrective action implementation by the responsible AU Manager. Plans for corrective actions will be documented and approved by the applicable AU Manager using the Corrective Action Plan template in enclosure (4).

9. Statement of Assurance

a. The Statement of Assurance (SOA) is a command-wide annual report that certifies the commanding officer's level of reasonable assurance as to the overall adequacy and effectiveness of internal controls within the command. The SOA is also used to disclose known management control accomplishments and deficiencies identified using MIC Program processes, and to describe plans and schedules to correct any reported management control deficiencies. The SOA reporting period begins 1 July and ends 30 June.

b. The submission of the command's SOA will be coordinated by the command MICP Coordinator.

c. The SOA submission will include the following:

1) Cover Memorandum. A cover memorandum signed by the SUPSHIP commanding officer shall provide senior management's assessment as to whether there is reasonable assurance that internal controls are in place and operating effectively. In addition, the SOA must certify to the number of management control reviews that are scheduled for the upcoming MIC year and the number of management control reviews completed during the previous MIC year. The certification must take one of the following three forms:

(a) An **unqualified statement of assurance** (reasonable assurance with no material weaknesses reported). Each unqualified statement shall provide a firm basis for that position, which the Agency Head (or principal deputy) will summarize in the cover memorandum.

(b) A **qualified statement of assurance** (reasonable assurance with exception of one or more material weaknesses noted). The cover memorandum must cite the material weaknesses in internal controls that preclude an unqualified statement.

(c) A **statement of no assurance** (no reasonable assurance because no assessments conducted or the noted material weaknesses are pervasive). The commanding officer shall provide an extensive rationale for this position.

2) Accomplishments. This is a brief summary of the most significant accomplishments and actions taken by the command during the SOA reporting period to strengthen internal controls. The accomplishments shall be ordered by significance with the most significant accomplishments listed first. Management control accomplishments may include improved compliance with laws and regulations, improvements in protection of Government property, improved efficiency of operations, and increased conservation of command resources.

3) Listing of all internal control deficiencies. This will include all uncorrected and corrected Material Weaknesses (MW), Reportable Conditions (RC), and Items to be Revisited (IR). A Material Weakness is a management control deficiency, or collection of management control deficiencies, which is significant enough to report to the next higher level. The determination is a management judgment as to whether a weakness is material. A Material Weakness impairs or may impair the ability of an organization to fulfill its mission or operational objective. A Reportable Condition is a control deficiency, or combination of control deficiencies, that adversely affects the ability to meet mission objectives but are not deemed by the Head of the Component as serious enough to report as material weaknesses. An Item to be Revisited is a management control deficiency where insufficient data exists to determine whether the deficiency constitutes an MW or RC.

4) Detailed narrative descriptions of all uncorrected MW, RC, and IR including the plans and schedules for corrective actions. This should include those identified during the current year and those disclosed in prior years with updated corrective action information.

5) Detailed narrative descriptions of all corrected MWs, RCs, and IRs identified during prior reporting periods.

d. All AU Managers will provide input to the command SOA by submitting a signed memorandum providing reasonable assurance that the system of internal controls, applicable to their assigned AU's, in place during the current SOA reporting period, are adequate and effective. The template to be used by all AU Managers is contained in enclosure (5). Internal Control accomplishments and deficiencies that meet the definition in paragraph 9.c.2 and 9.c.3 respectively should be described in detail. At the MICP Coordinator's discretion, enclosure (6), the AU Accomplishments form and enclosure (7), the New AU Deficiency Form, may be used for these descriptions.

Prior to submission of enclosure (5), all AUMs must submit a certification package which includes the following:

1. Management Control Review
2. AU Risk Assessment
3. AU Internal Control Assessment
4. AUM Certification Statement
5. New Deficiency Form

10. SUPSHIP MICP Configuration Control Board (CCB)

a. This manual establishes the SUPSHIP MICP Configuration Control Board (CCB). The MICP CCB will be chaired by NAVSEA 04Z and CCB members will include all SUPSHIP MICP Coordinators. Configuration control is essential to ensuring that policies, procedures, methodologies, and forms usage mandated by this manual are not deviated from without prior review and approval by the SUPSHIP MICP CCB.

b. SUPSHIP MICP CCB concurrence and approval is required for the following:

- Deviation from use of standardized documentation
- Modifications to AU Inventory
- Deviation from any other procedures and methodologies mandated by this manual

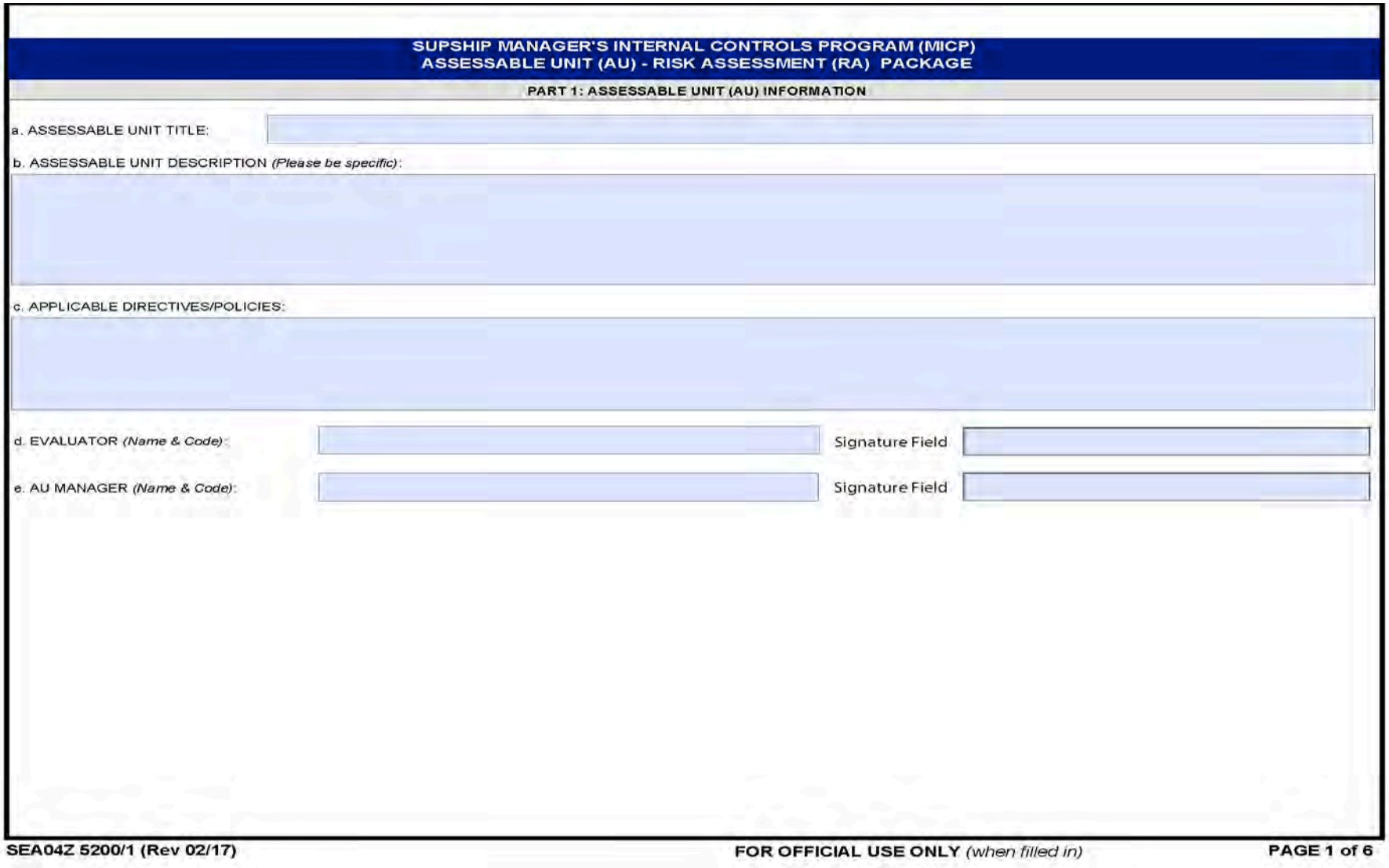
c. Proposed changes to this manual should be submitted to the SUPSHIP MICP CCB and all team members for review, discussion, and approval prior to implementation of any proposed changes. Control of proposed changes is performed under the auspices of SUPSHIP MICP CCB, who will consider all impacts of incorporating the recommended change prior to approval.

d. The SUPSHIP MICP CCB will conduct teleconferences on an as needed basis to discuss MICP changes which require CCB approval as described in paragraph 10(b) of this manual and to discuss MICP-related matters.

Enclosure 1 – Sample Assessable Unit Inventory

Sample FY 2017 Assessable Unit Inventory					
Major AU Name	**SUPSHIP Common**	**Sub AU's**	**AU Definition**	**AU Manager/Assessor**	**Status**
			(01) Communications		
Command Relationships and Communication	√	Command Communication - Internal	Internal communication is communication by a military organization with service members, civilian employees, retirees, and family members of the organization that creates an awareness of the organization's goals and activities, informs them of significant developments affecting them and the organization, increases their effectiveness as ambassadors of the organization, and keeps them informed about what is going on in the organization. Six elements to address are: link sailors and their leaders through a free flow of news and information, help sailors understand their roles in the Navy mission, explain how policies, programs and operations affect Navy members, promote good citizenship and foster pride, recognize individual and team achievements, and provide avenues for feedback.	**Kristin Mason**	Current/Mandatory
	√	Command Communication - External	The release of information and communicating to the public at large, ensuring proper handling of public information and that media have access to the information they need to report on military activities. External communication is also the establishment of strong community outreach that fosters good communication and relations between military and civilian communities.	**Kristin Mason**	Current/Mandatory
	√	Strategic Planning	A management process used to adequately plan for the future, set priorities, allocate resources, assess operations effectiveness, and establish goals with desired results.		Current
			(09) Manufacturing, Maintenance & Repair		
Environmental Programs	√	Environmental, Safety & Health	Administration of SUPSHIP's environmental, safety, and health program including the evaluation of contractor programs to ensure a safe work place and prevent industrial accidents.	**Teresa Bartolini**	Current/Mandatory
Ocupational Safety and Health (OSH)	√			**Teresa Bartolini**	Current/Mandatory
Calibration and Metrology	√				New/Mandatory
Engineering Technical Authority	√		Technical Authority is the authority, responsibility, and accountability to establish, monitor and approve technical standards, tools, and processes in conformance with higher authority policy, requirements, architectures and standards. The exercise of Technical Authority is a process that establishes and assures adherence to technical standards and policy providing a range of technically acceptable alternatives with risk and value assessments. The Waterfront Chief Engineer is responsible and accountable to lead and focus our technical efforts from the waterfront to support and execute oversight for design, construction, modernization, maintenance and repair. This includes investigating and resolving construction engineering problems and coordinating technical directorate actions for ship key events.	**Rick Warren** Andy Jordan	Current
Dry Dock Operations			Process of removing a ship from its normal waterborne environment or placing in a waterborne environment for the first time, via a marine railway, floating dry-docking, graving dock or building ways. Program designed to ensure safety of US Navy ships which are dry-docked or launched.	**Rick Warren** Kathi Dubar	Current (Bath only)
			NAVSEA Approved Waivers		
Total Force Implications	√	Equal Employment Opportunity			New/Mandatory Waiver Approved
Total Force Implications	√	Hazing Compliance & Training			New/Mandatory Waiver Approved
Personnel and Organizational Management	√	Command IA Coordinator			New/Mandatory Waiver Approved

Enclosure 2 – Assessable Unit Risk Assessment Form



SUPSHIP MANAGER'S INTERNAL CONTROLS PROGRAM (MICP)
ASSESSABLE UNIT (AU) - RISK ASSESSMENT (RA) PACKAGE

PART 1: ASSESSABLE UNIT (AU) INFORMATION

a. ASSESSABLE UNIT TITLE:

b. ASSESSABLE UNIT DESCRIPTION *(Please be specific)*:

c. APPLICABLE DIRECTIVES/POLICIES:

d. EVALUATOR *(Name & Code)*: Signature Field

e. AU MANAGER *(Name & Code)*: Signature Field

SEA04Z 5200/1 (Rev 02/17) **FOR OFFICIAL USE ONLY** *(when filled in)* **PAGE 1 of 6**

PART 2: LIST UP TO 5 OF THE MOST SEVERE RISKS/FAILURES

Identify Risk(s)/Failure(s). For this Assessable Unit, Identify up to 5 of the most significant risks that could negatively impact command resources, mission and/or image **assuming no controls exist or the controls have failed**.

The risk assessment process is typically described in the format of an IF/THEN statement e.g., "IF personal identifiable information (PII) is mishandled, THEN employee identities could be stolen." Where "mishandling of PII" is what we try to prevent from happening by putting in controls, "identity theft" is the impact to the command of not mitigating the **RISK/FAILURE**.

LIST UP TO 5 OF THE MOST SEVERE RISKS/FAILURES HERE:

R1	SHORT TITLE: DESCRIPTION:
R2	SHORT TITLE: DESCRIPTION:
R3	SHORT TITLE: DESCRIPTION:
R4	SHORT TITLE: DESCRIPTION:
R5	SHORT TITLE: DESCRIPTION:

SEA04Z 5200/1 (Rev 02/17) **FOR OFFICIAL USE ONLY** *(when filled in)* **PAGE 2 of 6**

PART 3: INHERENT AND CONTROL RISK RATINGS

Complete the Risk Assessment, for each risk/failure identified in Part 2. Using your subject matter expertise, rate the Inherent Risk (Step 1) and the Control Risk (Step 2) based on the rating descriptions provided.

STEP 1: INHERENT (CONSEQUENCE) RISK RATING

Complete the Inherent Risk table for each Risk (R1-R5) to determine the impact assuming controls do not exist or have failed. Determine the rating for each of the seven Inherent Risk Categories that is applicable or significant to the risk being assessed. For each risk, read the description for each Inherent Risk Category and enter the rating number (1, 2, 3, 4 or 5) that best describes the inherent risk rating, **assuming controls don't exist or have failed**. If a risk category is not applicable or not significant to the risk being assessed, either enter "0" or leave the entry blank.

The highest rating number from each rating column appears in the Highest Inherent Risk Ratings (bottom row) and will be used on page 6 to determine the Combined Risk.

STEP 2: CONTROL (LIKELIHOOD) RISK RATING

When determining the Control Risk, consider the likelihood of a failure occurring assuming **all current controls are in place**. Note that controls are in place to reduce the likelihood that the process will fail.

Complete the Control Risk Rating table for each Risk (R1-R5) to determine the likelihood that a risk will occur despite the controls in place. Determine the rating for each of the four Control Risk Categories listed in the first column of the table. For each category, read the description provided and enter the rating number (1, 2, 3, 4 or 5) that best describes the probability of each risk occurring **assuming all controls are in place and functioning**.

Note that the higher rating for each category indicates greater likelihood of the risk or failure occurring. Like the weakest link that establishes the strength of a chain, the likelihood category that has the highest rating establishes the greatest probability of the risk or failure occurring.

The highest rating number from each rating column appears in the Highest Control Risk Ratings (bottom row) and will be used with the highest Inherent Risk Ratings on page 6 to determine the Combined Risk.

SEA04Z 5200/1 (Rev 02/17) **FOR OFFICIAL USE ONLY** *(when filled in)* **PAGE 3 of 6**

INHERENT RISK RATING

RISK/FAILURE: *for the full risk verbiage see page 2*	R1	
	R2	
	R3	
	R4	
	R5	

Inherent Risk Category	Rating 1 (No discernible impact)	Rating 2 (Minor Impact)	Rating 3 (Moderate Impact)	Rating 4 (Severe Impact)	Rating 5 (Unacceptable)	INHERENT RISK RATINGS				
						R1	R2	R3	R4	R5
Visibility	No report of corrective action up the chain is required.	A division-level investigation and corrective action is required.	A department-level investigation and corrective action is required.	A formal command-level investigation is required.	A formal external investigation is required or potential outcome could make it into the news media.					
Work Stoppage	Process would not be stopped.	Process would be temporarily stopped with little or no cost impact.	Process would be temporarily stopped with medium cost impact.	Process would be stopped with broad cost impact.	There would be a loss of authority to operate process.					
Containment	Distribution of faulty product or information spill is limited to the division.	Distribution of faulty product or information spill is limited to the department.	Distribution of faulty product or information spill is limited to the NAVSEA.	Distribution of faulty product or information spill is not limited to the DoN, but is known.	Distribution of faulty product or information spill is not limited to the DoN or is unknown.					
Discipline	No disciplinary action would be taken.	Moderate isolated disciplinary action likely.	Moderate disciplinary action likely for several employees.	Isolated serious disciplinary action likely.	Serious disciplinary action likely for several employees.					
Safety	No people would incur injuries, and no equipment/ plant damage.	Some people could incur minor injuries or equipment/plant damage would be up to $25K.	Some people could incur moderate injuries or equipment/plant damage would be $25K to $100K.	Some people could incur serious injury or equipment/plant damage would be $100K to $1M.	Someone could suffer permanent injury or be killed or equipment/ plant damage would be >$1M.					
Process Output Quality	Process output quality is not impacted.	Process output meets minimum requirements, but can be improved.	Process output will meet most, but not all minimum requirements.	Process output will not meet most of the minimum requirements.	Process output will not meet any of the minimum requirements.					
Milestone Timeliness	There are no time-sensitive milestones or there are and they are completed ahead of schedule.	Time-sensitive milestones are completed on time.	Time-sensitive milestones are completed late, but time can be recovered later in the process.	Time-sensitive milestones are completed late and time cannot be recovered.	Milestones are not completed.					
					Highest Inherent Risk Ratings					

SEA04Z 5200/1 (Rev 02/17) **FOR OFFICIAL USE ONLY** *(when filled in)* **PAGE4 of 6**

CONTROL RISK RATING

RISK/FAILURE: *for the full risk verbiage see page 2*	R1	
	R2	
	R3	
	R4	
	R5	

Control Risk Category	Rating 1 (Not Likely) ~10% probability of Risk occurring	Rating 2 (Low Likelihood) ~30% probability of Risk occurring	Rating 3 (Likely) ~50% probability of Risk occurring	Rating 4 (Highly Likely) ~70% probability of Risk occurring	Rating 5 (Near Certainty) ~90% probability of Risk occurring	CONTROL RISK RATINGS R1	R2	R3	R4	R5
Documentation	• Users know and understand the process • Process is documented • Controls are documented, understandable, and usable • There is configuration control of the document • Users know where and how to access the documentation	• Users know and understand the process • Process is documented • Controls are documented, understandable, and usable • There is configuration control of the document	• Users know and understand the process • Process is documented • Controls are documented, understandable, and usable	• Some users know and understand the process • Controls are partially effective	• Users do not know or understand the process • Controls are ineffective					
Responsibilities	• People know their responsibilities • People are adequately trained • Training is monitored and tracked • People have needed resources to accomplish responsibilities • Adequate Staff	• People know their responsibilities • People are adequately trained • Training is monitored and tracked • Minimally Adequate Staff	• People know what their responsibilities are • People are adequately trained • Limited Staff	• People not fully executing responsibilities • Very Limited Staff	• People do not know their responsibilities • No Staff					
Internal Reviews	• Processes are reviewed annually • Controls are tested when process changes are made • Compliance reviews are conducted annually • Risk assessments are performed annually • Controls are tested periodically • Test results are documented	• Processes are reviewed annually • Controls are tested when process changes are made • Compliance reviews are conducted annually • Risk assessments are performed annually • Controls are tested periodically	• Processes are reviewed annually • Controls are tested when process changes are made • Compliance reviews are conducted annually	• Processes are reviewed annually • Occasional incidents of non-compliance	• Processes are not reviewed annually • Frequent incidents of non-compliance					
Continuous Process Improvement	• Past failures are reported • Past failures or process improvement recommendations are documented • Corrective action or improvement plans are established • Corrective actions or improvement plans are monitored to effective completion	• Past failures are reported • Past failures or process improvement recommendations are documented • Corrective action or improvement plans are established	• Past failures are reported • Past failures or process improvement recommendations are documented	• Past failures are reported • Partial/ inadequate corrective action	• Past failures are not reported • No corrective actions taken					
					Highest Control Risk Ratings					

SEA04Z 5200/1 (Rev 02/17) **FOR OFFICIAL USE ONLY** *(when filled in)* **PAGE 5 of 6**

PART 4: DETERMINING THE COMBINED RISK RATING

For each Risk (R1-R5), the Inherent Risk and Control Risk ratings from pages 4 and 5 are plotted below on the Combined Risk Matrix. The Inherent Risk ratings are plotted on the horizontal axis and the Control Risk ratings are plotted on the vertical axis. The Combined Risk color (green - low, yellow - moderate, high - red) is then shown in the table below for each risk.

Review the results of each Risk on the Combined Risk Matrix to ensure accuracy.

Final step: AU Manager assigns an overall risk assessment by selecting Low, Moderate or High from the drop-down list in the AU Manager's Overall Risk Assessment box below. This assessment will typically correspond to the highest risk shown in the Combined Risk column. The AU Manager may elect to provide an overall assessment that is higher or lower than the highest Combined Risk level, but should be prepared to justify this action.

RISK/FAILURE:		
for the full risk verbiage see page 2	R1	
	R2	
	R3	
	R4	
	R5	

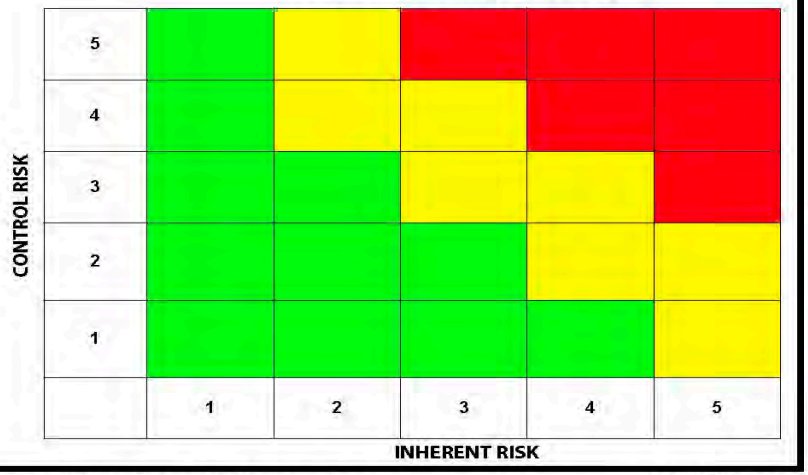
	INHERENT RISK	CONTROL RISK	COMBINED RISK
R1			
R2			
R3			
R4			
R5			

AU MANAGER'S OVERALL RISK ASSESSMENT (Low, Moderate, High)

COMBINED RISK KEY

Low	Moderate	High

COMBINED RISK MATRIX



SEA04Z 5200/1 (Rev 02/17) **FOR OFFICIAL USE ONLY** *(when filled in)* **PAGE 6 of 6**

Enclosure 3A – AU Internal Control Assessment Summary (Excel format)

Assessable Unit (AU) - Internal Control Assessment Summary									
Part 1: Assessable Unit Information									
Assessable Unit Name:									
Assessable Unit Manager:									
Assessable Unit Description: *(The AU description should be written in a way so that anyone unfamiliar with the program/process will understand it. It should be clear and concise.)*									
Instructions/Guidance: *(List all applicable directives/policies that govern the AU.)*									
Assessable Unit Risk Level: *(From the AU Manager's Overall Risk Asessment rating on page 6 of the AU Risk Assessment Form, SEA 04Z 5200/1)*									
Accomplishments: *(Highlight areas where you have became more effective or efficient in operations, improved fiscal stewardship, or complied with applicable laws and regulations.)*									
Part 2: Internal Control Assessment									
Risks	**Inherent Risk Level**	**Control Risk Level**	**Combined Risk Level**	**Internal Controls**	**Validation**	**Date Conducted**	**Weaknesses &Deficiencies**	**Corrective Action**	**Target Resolution Date**
Probable or potential adverse events or conditions that may result in loss of resources, failure to accomplish mission or mismanagement.	Risk level assuming no controls exist or controls have failed	Likelihood that an error or problem will occur and not be prevented or detected by internal control	Risk considering both likelihood of failure and potential impact	The organization, policies, procedures, techniques, and mechanisms that enforce management directives. Internal Controls ensure reasonable assurance of 1) effectiveness & efficiency; 2) reliability or reporting for internal and external use; 3) compliance with laws and regulations; 4) assets are safeguarded from loss or misuse.	Tangible proof that internal controls are working as intended (OQE).		Lack of an internal control where necessary, or existing internal controls are found to not be functioning as intended.	Explain how you will validate that the weakness or deficiency no longer exists and validate actions taken. The Corrective action should also describe the steps and associated timelines necessary to correct the weakness or deficiency.	

INHERENT RISK LEVELS

Low: AU Manager believes the potential risk does not have severe consequences and is unlikely to occur.

Moderate: AU Manager believes the potential risk has severe consequences or is likely to occur.

High: AU Manager believes the potential risk has severe consequences and is likely to occur.

INHERENT RISK LEVELS

Low: AU Manager believes the potential risk does not have severe consequences and is unlikely to occur.

Moderate: AU Manager believes the potential risk has severe consequences or is likely to occur.

High: AU Manager believes the potential risk has severe consequences and is likely to occur.

COMBINED RISK LEVELS

Low: AU Manager believes likelihood of hazard or process failure does not pose significant threat to mission, resources, or image.

Moderate: AU Manager believes potential for a hazard or process failure suggests greater attention needed monitoring or improving controls.

High: AU Manager believes likelihood of significant hazard or process failure suggests implementation of effectve controls is imperative

Enclosure 3B – AU Internal Control Assessment Summary (PDF format)

Assessable Unit (AU) - Internal Control Assessment Summary

Part 1: Assessable Unit Information

1. **Assessable Unit Name:**
2. **Assessable Unit Manager/Code:**
3. **Assessable Unit Description:** *(The AU description should be clear, concise and written so anyone unfamiliar with the program/process will understand it.)*
4. **Instructions/Guidance:** *(List all applicable directives/policies that govern the AU.)*
5. **Assessable Unit Overall Risk Level:** *(From the AU Manager's Overall Risk Assessment rating on page 6 of the AU Risk Assessment Form, SEA 04Z 5200/1)*
6. **Accomplishments:** *(Highlight area where you have become more effective or efficient, improved fiscal stewardship, or corrective actions have reduced Control Risk.)*

Part 2: Internal Control Assessments

Risks	Inherent Risk Level	Control Risk Level	Combined Risk Level	Internal Controls	Validation	Date of Valid.	Weaknesses & Deficiencies	Corrective Action	Target Date	Add
										Del
										Del
										Del
										Del
										Del
										Del
										Del
										Del
										Del

SEA04Z 5200/3 (Rev 02/17) **FOR OFFICIAL USE ONLY** *(when filled in)* **PAGE 1 of 1**

Enclosure 4 – Management Control Review Form

SUPSHIP MANAGEMENT CONTROL REVIEW FORM

1. ASSESSABLE UNIT (AU) TITLE:

2. EVALUATION CONDUCTED BY:

a. NAME *(Last, First, Code)*: b. DATE OF EVALUATION:

3. IDENTIFY CONTROL BEING ASSESSED AND ASSOCIATED RISK(S):

a. CONTROL: ◯AUTOMATED ◯MANUAL b. RISK(S):

4. IDENTIFY CONTROL TYPE *(Check one)*:

PREVENTIVE ◯	DETECTIVE ◯	DIRECTIVE ◯	CORRECTIVE ◯
Preventive controls deter undesirable events from occurring. Preventive controls should be designed to discourage errors and irregularities from occurring.	Detective controls detect and correct undesirable events that occurred. Detective controls should be designed to identify an error or irregularity after it has occurred.	Directive controls cause or encourage a desirable event to occur. Directive controls should be designed to assist in accomplishing goals and objectives.	Corrective controls are aimed at restoring the system to its expected state. Corrective controls can terminate the affected process, reverse the error, or remedy the results of the error.
Examples include: • Standard Operation Procedures (SOPs) • Monitoring mechanisms • Quality Control (QC) • Computer applications that check the transactions	Examples include: • Manager's review of logs • Comparison of actual vs.expected • Audits & Surveillances • Quality Assurance (QA)	Examples include: • Directives, Instructions, Regulatory, & Requirements Manuals • Training Seminars • Written job descriptions	Examples include: • Back-up files or hard drive images that can be restored to a prior state • Budget variance reports • In an Internet-enabled environment, a transaction trail or log to follow up and correct the damage

5. METHOD OF TESTING KEY CONTROLS *(Check all that apply)*:

a. DIRECT OBSERVATION ☐	b. FILE/DOCUMENTATION REVIEW ☐	c. ANALYSIS ☐	d. SAMPLING ☐
e. SIMULATION ☐	f. INTERVIEWS ☐	g. OTHER *(Explain)* ☐	

6. ASSESSMENT RESULTS:

Is the control working as intended? How do you know if it is not? Give specifics. *(e.g., if control is a document review, the assessment would pull a sample (give sample size) and report on the number of errors that weren't caught by review.)*

Page 1 of 2

SUPSHIP MANAGEMENT CONTROL REVIEW FORM

7. INTERNAL CONTROL DEFICIENCIES/WEAKNESSES DETECTED, IF ANY:

8. CORRECTIVE ACTIONS *(If applicable)*:

AU Manager provide description of corrective actions planned and/or completed and an estimated completion date for each deficiency/weakness. Submit applicable objective quality evidence (OQE).

9. CERTIFICATION AND SIGNATURE:

I certify that the internal control for this Assessable Unit has been evaluated in accordance with the provisions established by the Managers' Internal Control Program. This certification statement and any supporting documentation will be provided to the AU Manager and MIC Program Coordinator.

a. EVALUATOR NAME:	b. EVALUATOR SIGNATURE:
c. AU MANAGER NAME AND CODE:	d. AU MANAGER SIGNATURE:

Page 2 of 2

Enclosure 5 – Sample Statement of Assurance

Certification Statement

25 Dec 2016

MEMORANDUM

From: AU Manager
To: Code 100
Via: *Code 100B*

Subj: STATEMENT OF ASSURANCE CERTIFICATION STATEMENT

Ref: (a) Certification Package

1. I have reviewed the system of internal controls in effect for the period of 1 April 2015 through 30 March 2016 for Code xxx applicable assessable units. All internal control accomplishments and internal control deficiencies identified between 1 April 2015 and 30 March 2016 are contained in reference (a). Plans for corrective action, where applicable, are also contained in reference (a).

2. With the exception of any deficiencies identified in reference (a), I have reasonable assurance that internal controls are in place and operating effectively, and that the objectives of the Federal Financial Managers' Integrity Act were achieved.

3. Information to support this certification statement was derived from reviews, audits, inspections, observations, knowledge gained from daily operations of programs, and/or other methods that evaluate internal controls.

J. D. Doe

Enclosure 6 – AU Accomplishments

(Optional at MICP Coordinator's Discretion)

Assessable Unit Name

ACQUISITION STAFFING (DAWIA) TRAINING PROCESS

Description: The process of providing for all SUPSHIP acquisition training and employee development.

Standards: DON DAWIA Operating Guide

2016-2017 Internal Control Accomplishments

(Explain Accomplishments Below)

2016-2017 Internal Control Deficiencies

(Explain Deficiency Below)

Plans for Corrective Action

(Explain plans to correct above deficiencies)

Enclosure 7 – New AU Deficiency Form

(Optional at MICP Coordinator's Discretion)

1. Title of Deficiency

2. Description of Deficiency

3. Year Identified

4. Original Targeted Correction Date

5. Current Target Date

6. Validation Process

7. Results Indicator

8. Source(s) Identifying Deficiency

9. Planned Milestones:

a. Current Fiscal Year

b. Next Fiscal Year
