

# **Chapter 2 – Standards of Conduct and Managers’ Internal Control Program (MICP)**

## **Table of Contents**

<b>2.1</b>	<b>Introduction</b>	<b>2-3</b>
<b>2.2</b>	<b>Summary of Amended Procurement Integrity Act</b>	<b>2-3</b>
<b>2.3</b>	<b>Disclosing and Obtaining Procurement Information</b>	<b>2-4</b>
2.3.1	Disclosing Procurement Information	2-4
2.3.2	Obtaining Procurement Information	2-4
<b>2.4</b>	<b>Actions Required Regarding Offers of Non-Federal Employment</b>	<b>2-4</b>
<b>2.5</b>	<b>Post-Government Employment Restrictions</b>	<b>2-5</b>
<b>2.6</b>	<b>Determining Violations or Possible Violations</b>	<b>2-6</b>
<b>2.7</b>	<b>Measures to Minimize Improper Conduct</b>	<b>2-6</b>
<b>2.8</b>	<b>Hotline Policies and Procedures for NAVSEA Shore Activities</b>	<b>2-7</b>
<b>2.9</b>	<b>Fraud, Waste, and Other Abuse</b>	<b>2-8</b>
2.9.1	Coordination for Fraud Prevention	2-8
2.9.2	Indicators of Defective Pricing Fraud	2-8
2.9.3	Actions against Fraudulent Activities	2-10
2.9.4	Government Personnel	2-11
<b>2.10</b>	<b>Managers’ Internal Control Program (MICP)</b>	<b>2-11</b>
	<b>Appendix 2-A: Acronyms</b>	<b>2-13</b>
	<b>Appendix 2-B: SUPSHIP Managers’ Internal Control Program (MICP) Manual</b>	<b>2-15</b>

## **References**

- (a) 5 CFR 2635, Standards of Ethical Conduct for Employees of the Executive Branch
- (b) DoD 5500.7-R, DoD Joint Ethics Regulations
- (c) 41 USC 421, Office of Federal Procurement Policy Act
- (d) PL 104-106, Amended Procurement Integrity Act
- (e) Federal Acquisition Regulations (FAR)
- (f) 5 CFR 2641, Post-Employment Conflict of Interest Restrictions
- (g) DoD Directive 5500.07, DoD Standards of Conduct
- (h) NAVSEAINST 5041.1A, 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 5430.92B, Assignment of Responsibilities to Counteract Acquisition Fraud, Waste, and Related Improprieties within the Department of the Navy
- (k) 31 USC 3729, Civil False Claims Act
- (l) 31 USC 3801, Program Fraud Civil Remedies Act
- (m) 41 USC 601-613, Contract Disputes Act
- (n) 41 USC 51- 58, Anti-Kickback Act of 1986
- (o) 41 USC 605, Decision by contracting officer
- (p) 10 USC 2408, Prohibition on Persons Convicted of Defense Contract-Related Felonies and Related Criminal Penalty on Defense Contractors
- (q) 10 USC 2324, Allowable Costs Under Defense Contracts
- (r) OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control
- (s) NAVSEAINST 5200.13D, Managers' Internal Control Program

### **SUPSHIP Managers' Internal Control Program Manual**

- (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) DoD Instruction 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

## Chapter 2 – Standards of Conduct and Managers’ Internal Control Program (MICP)

### 2.1 Introduction

Considering the significant power vested in Government officials, the public should expect the conduct of such officials to conform to the highest ethical standards. Congress has passed numerous ethics laws, and the Executive branch has promulgated Government-wide regulations addressing the standards of ethical conduct expected of Government employees, both military and civilian (see [5 CFR 2635](#), reference (a), Standards of Ethical Conduct for Employees of the Executive Branch and [DoD 5500.7-R](#), reference (b), the DoD Joint Ethics Regulations). As required by DoD for its employees, SUPSHIP personnel receive periodic ethics training from their local counsel’s office.

In the context of federal procurements, Congress enacted the Office of Federal Procurement Policy Act, [41 USC 421](#), reference (c). This law was amended by [Public Law 104-106](#), reference (d), and is referred to as the Amended Procurement Integrity Act.

### 2.2 Summary of Amended Procurement Integrity Act

[FAR 3.104](#), reference (e), implements section 27 of the Office of Federal Procurement Policy Act ([41 USC 423](#)). The effective date of the new law was 1 January 1997. The amended law focuses on:

- 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

These items will be discussed in more detail in later sections of this chapter.

The amended law eliminates all requirements for written certifications, e.g., certifications regarding familiarity with the act; not being aware of violations; promising to disclose information about possible violations; and continuing obligation not to disclose proprietary and source selection information.

The amended law eliminates the prior prohibition on a “procurement official” soliciting or accepting a gratuity valued at more than \$10 from a “competing contractor” “during the conduct of a procurement.” This restriction was deemed to duplicate other gratuities rules, such as the prohibition in the Government-wide standards of conduct regarding gifts from prohibited sources in excess of \$20.

Further, the amended law eliminates the requirement for each agency to have a procurement ethics program for training its procurement officials.

## **2.3 Disclosing and Obtaining Procurement Information**

### **2.3.1 Disclosing Procurement Information**

The amended law prohibits certain persons from disclosing certain procurement information, i.e., contractor bid or proposal information or source selection information. 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

Such persons must not knowingly disclose such information before the award of the procurement to which the information relates. This section applies only to procurements using competitive procedures. The amended 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.

Definitions relative to this prohibition, “source selection and proprietary information,” are essentially the same terms as prior to amending of the law. The term “contractor bid or proposal information” encompasses proprietary information.

### **2.3.2 Obtaining Procurement Information**

The amended law also prohibits anyone from knowingly obtaining the procurement information described above. Specifically, no one will knowingly obtain such information before award. Mere solicitation of procurement information does not violate the amended law. The same criminal penalties apply to knowingly obtaining procurement information.

## **2.4 Actions Required Regarding Offers of Non-Federal Employment**

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, he or she will give notice and disqualify him or herself from participating in the procurement, unless the possibility of employment is rejected.

The official must report this contact in writing to the immediate supervisor and to the Designated Agency Ethics Official (DAEO), or his designee (local counsel), and either reject the possibility of employment or disqualify himself/herself from further participation until authorized to resume participation. In contrast to the prior law, the disqualification is immediate.

A written notice of disqualification goes to the Head of the Contracting Activity (HCA) or his/her 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.

FAR states that if an employee participates “personally and substantially” in certain listed procurement-related activities, then he/she will be required to report such contacts and either reject the possibility of employment or disqualify himself/herself. 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.

## 2.5 Post-Government Employment Restrictions

The amended law 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. However, the amended law only applies to services provided or decisions made on or after 1 January 1997, the effective date of the amended law.

Individuals who left the Government prior to 1 January 1997 are not covered by the amended law, but are subject to the old procurement integrity rules. However, the old procurement integrity rules do not apply to anyone after 31 December 1998.

Under the amended law, a former agency official may not accept compensation from a contractor within a period of one year after such official:

- Served 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.
- Served 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 made 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
  - 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.

Under the amended law, as under the old law, the DAEO (counsel) 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 post-government employment restriction, the term “in excess of \$10 million” means the value of a contract, including the estimated value of the contract at the time of award, and all options.

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

## **2.6 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 the violation or possible violation impacts the procurement, he/she is to forward this information to the HCA or his/her designee. The HCA who receives information that describes an actual or possible violation will review all relevant information and take appropriate action. The HCA may request information from appropriate parties about the violation. 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.

## **2.7 Measures to Minimize Improper Conduct**

SUPSHIP personnel should be familiar with the requirements of FAR 3.104, [DoDD 5500.07](#) (Standards of Conduct), reference (g), 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.

SUPSHIP should analyze and identify operations with particular 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 of Government personnel at remote contractor's sites through unscheduled inspections of specific operations by military or civilian supervisors
- 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

## **2.8 Hotline Policies and Procedures for NAVSEA Shore Activities**

[NAVSEAINST 5041.1A](#), reference (h), applicable to all NAVSEA shore activities and detachments, encourages employees to use the chain of command in reporting fraud or relating improprieties. Otherwise, employees are encouraged to use the local Hotline, or NAVSEA, Navy, or DoD Hotlines.

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

## 2.9 Fraud, Waste, and Other Abuse

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

### 2.9.1 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 ensure establishment of a centralized point 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 will be able to use its 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 5430.92B](#), 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 acquisition activities affecting the DoN. 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.

### 2.9.2 Indicators of Defective Pricing Fraud

Auditors assess pricing situations to determine if the circumstances surrounding any positive defective pricing are indicators of potential fraud. The auditor is responsible for finding and reporting indicators, not proving fraud. The Truth-in-Negotiations Act 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 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
- 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

### **2.9.3 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 USC 3729](#), reference (k), 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 USC 3801](#) (as amended by [Public Law 110-69](#)), reference (l), allows Federal agencies to impose administrative penalties for certain false claims and statements.

The Contract Disputes Act, [41 USC 601-613](#), reference (m), 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](#)) and [41 USC 51-58](#), the Anti-Kickback Act of 1986, reference (n), 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.

According to [41 USC 605](#), reference (o), 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](#) 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.

By provisions of [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.

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](#), reference (p), provides guidelines on "Prohibition on Persons Convicted of Defense Contract-Related Felonies and Related Criminal Penalty on Defense Contractors." Among other things, the statute 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](#), reference (q), 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.

#### **2.9.4 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.

### **2.10 Managers' Internal Control Program (MICP)**

[OMB Circular A-123](#), Management's Responsibility for Enterprise Risk Management and Internal Control, reference (r), states that "Enterprise Risk Management (ERM) and Internal Control are 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 entity's oversight body,

management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved.”

[NAVSEAINST 5200.13D\\*\\*](#), Managers’ Internal Control Program, reference (s), states NAVSEA policy on internal controls and requires that all commands establish Managers’ Internal Control Programs (MICPs) to support commanders and managers in meeting the requirements of [OMB Circular A-123](#). The MICP is a tool to evaluate and report on the effectiveness of internal controls throughout an organization and to identify and, when necessary, take 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.

\*\* 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
FAR	Federal Acquisition Regulations
HCA	Head of the Contracting Activity
IR	Item to be Revisited
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
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
USC	United States Code

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

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

**2 April 2017**

# **Supervisor of Shipbuilding**

## **Managers' Internal Control Program (MICP)**

### **Manual**

#### **Table of Contents**

1. Purpose .....	2-18
2. Scope.....	2-18
3. Background.....	2-18
4. MICP Implementation.....	2-19
5. MICP Plan.....	2-19
6. Inventory of Assessable Units .....	2-20
7. Risk Assessment Process.....	2-21
8. Internal Control Assessment Documentation.....	2-23
9. Statement of Assurance .....	2-24
10. SUPSHIP MICP Configuration Control Board (CCB).....	2-26
Enclosure 1 – Sample Assessable Unit Inventory .....	2-28
Enclosure 2 – Assessable Unit Risk Assessment Form .....	2-29
Enclosure 3A – AU Internal Control Assessment Summary (Excel format) .....	2-35
Enclosure 3B – AU Internal Control Assessment Summary (PDF format).....	2-36
Enclosure 4 – Management Control Review Form .....	2-37
Enclosure 5 – Sample Statement of Assurance Certification Statement.....	2-39
Enclosure 6 – AU Accomplishments .....	2-40
Enclosure 7 – New AU Deficiency Form .....	2-41

## **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) DoD Instruction 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**

Table 1 – Levels of Inherent Risk and Control Risk .....	2-22
--	------

## 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/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**

<b>Risk</b>	<b>Low</b>	<b>Moderate</b>	<b>High</b>
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 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. Alternative Management Control Review (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 Alternative Management Control Review. 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
<b>(01) Communications</b>					
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
<b>(09) Manufacturing, Maintenance &amp; Repair</b>					
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
Occupational 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 Dobar	Current (Bath only)
<b>NAVSEA Approved Waivers</b>					
Total Force Implications	√	Equal Employment Opportunity			New/Mandatory Waiver Approved
Total Force Implications	√	Hazing Compliance & Training			New/Mandatory Waiver Approved
Persomel 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:	<input type="text"/>		
b. ASSESSABLE UNIT DESCRIPTION <i>(Please be specific)</i> :	<input type="text"/>		
c. APPLICABLE DIRECTIVES/POLICIES:	<input type="text"/>		
d. EVALUATOR <i>(Name &amp; Code)</i> :	<input type="text"/>	Signature Field	<input type="text"/>
e. AU MANAGER <i>(Name &amp; Code)</i> :	<input type="text"/>	Signature Field	<input type="text"/>

PART 2: LIST UP TO 5 OF THE MOST SEVERE RISKS/FAILURES	
<p><b>Identify Risk(s)/Failure(s).</b> For this Assessable Unit, Identify up to 5 of the most significant risks that could negatively impact command resources, mission and/or image <b>assuming no controls exist or the controls have failed.</b></p> <p>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 <b>RISK/FAILURE.</b></p>	
LIST UP TO 5 OF THE MOST SEVERE RISKS/FAILURES HERE:	
R1	SHORT TITLE: <div style="border: 1px solid black; height: 20px; width: 100%; background-color: #d9e1f2;"></div> DESCRIPTION: <div style="border: 1px solid black; height: 100px; width: 100%; background-color: #d9e1f2;"></div>
R2	SHORT TITLE: <div style="border: 1px solid black; height: 20px; width: 100%; background-color: #d9e1f2;"></div> DESCRIPTION: <div style="border: 1px solid black; height: 100px; width: 100%; background-color: #d9e1f2;"></div>
R3	SHORT TITLE: <div style="border: 1px solid black; height: 20px; width: 100%; background-color: #d9e1f2;"></div> DESCRIPTION: <div style="border: 1px solid black; height: 100px; width: 100%; background-color: #d9e1f2;"></div>
R4	SHORT TITLE: <div style="border: 1px solid black; height: 20px; width: 100%; background-color: #d9e1f2;"></div> DESCRIPTION: <div style="border: 1px solid black; height: 100px; width: 100%; background-color: #d9e1f2;"></div>
R5	SHORT TITLE: <div style="border: 1px solid black; height: 20px; width: 100%; background-color: #d9e1f2;"></div> DESCRIPTION: <div style="border: 1px solid black; height: 100px; width: 100%; background-color: #d9e1f2;"></div>

### 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.

INHERENT RISK RATING										
RISK/FAILURE:  <i>for the full risk verbiage see page 2</i>	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				
						R 1	R 2	R 3	R 4	R 5
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					

CONTROL RISK RATING										
RISK/FAILURE:  <i>for the full risk verbiage see page 2</i>	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				
						R 1	R 2	R 3	R 4	R 5
<b>Documentation</b>	<ul style="list-style-type: none"> <li>Users know and understand the process</li> <li>Process is documented</li> <li>Controls are documented, understandable, and usable</li> <li>There is configuration control of the document</li> <li>Users know where and how to access the documentation</li> </ul>	<ul style="list-style-type: none"> <li>Users know and understand the process</li> <li>Process is documented</li> <li>Controls are documented, understandable, and usable</li> <li>There is configuration control of the document</li> </ul>	<ul style="list-style-type: none"> <li>Users know and understand the process</li> <li>Process is documented</li> <li>Controls are documented, understandable, and usable</li> </ul>	<ul style="list-style-type: none"> <li>Some users know and understand the process</li> <li>Controls are partially effective</li> </ul>	<ul style="list-style-type: none"> <li>Users do not know or understand the process</li> <li>Controls are ineffective</li> </ul>					
<b>Responsibilities</b>	<ul style="list-style-type: none"> <li>People know their responsibilities</li> <li>People are adequately trained</li> <li>Training is monitored and tracked</li> <li>People have needed resources to accomplish responsibilities</li> <li>Adequate Staff</li> </ul>	<ul style="list-style-type: none"> <li>People know their responsibilities</li> <li>People are adequately trained</li> <li>Training is monitored and tracked</li> <li>Minimally Adequate Staff</li> </ul>	<ul style="list-style-type: none"> <li>People know what their responsibilities are</li> <li>People are adequately trained</li> <li>Limited Staff</li> </ul>	<ul style="list-style-type: none"> <li>People not fully executing responsibilities</li> <li>Very Limited Staff</li> </ul>	<ul style="list-style-type: none"> <li>People do not know their responsibilities</li> <li>No Staff</li> </ul>					
<b>Internal Reviews</b>	<ul style="list-style-type: none"> <li>Processes are reviewed annually</li> <li>Controls are tested when process changes are made</li> <li>Compliance reviews are conducted annually</li> <li>Risk assessments are performed annually</li> <li>Controls are tested periodically</li> <li>Test results are documented</li> </ul>	<ul style="list-style-type: none"> <li>Processes are reviewed annually</li> <li>Controls are tested when process changes are made</li> <li>Compliance reviews are conducted annually</li> <li>Risk assessments are performed annually</li> <li>Controls are tested periodically</li> </ul>	<ul style="list-style-type: none"> <li>Processes are reviewed annually</li> <li>Controls are tested when process changes are made</li> <li>Compliance reviews are conducted annually</li> </ul>	<ul style="list-style-type: none"> <li>Processes are reviewed annually</li> <li>Occasional incidents of non-compliance</li> </ul>	<ul style="list-style-type: none"> <li>Processes are not reviewed annually</li> <li>Frequent incidents of non-compliance</li> </ul>					
<b>Continuous Process Improvement</b>	<ul style="list-style-type: none"> <li>Past failures are reported</li> <li>Past failures or process improvement recommendations are documented</li> <li>Corrective action or improvement plans are established</li> <li>Corrective actions or improvement plans are monitored to effective completion</li> </ul>	<ul style="list-style-type: none"> <li>Past failures are reported</li> <li>Past failures or process improvement recommendations are documented</li> <li>Corrective action or improvement plans are established</li> </ul>	<ul style="list-style-type: none"> <li>Past failures are reported</li> <li>Past failures or process improvement recommendations are documented</li> </ul>	<ul style="list-style-type: none"> <li>Past failures are reported</li> <li>Partial/ inadequate corrective action</li> </ul>	<ul style="list-style-type: none"> <li>Past failures are not reported</li> <li>No corrective actions taken</li> </ul>					
					Highest Control Risk Ratings					

**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.

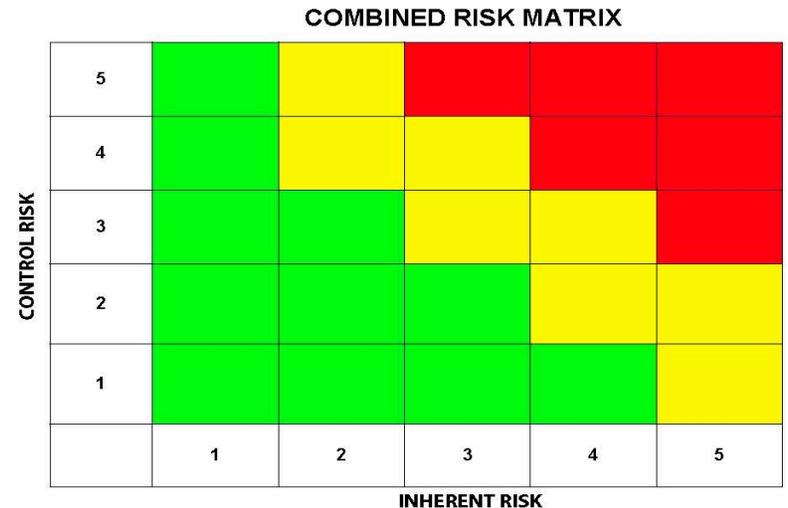
Review the results of each Risk on the Combined Risk Matrix to ensure accuracy.

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:	R1	
<i>for the full risk verbiage see page 2</i>	R2	
	R3	
	R4	
	R5	

INHERENT RISK	CONTROL RISK	COMBINED RISK
R1 <input type="text"/>	R1 <input type="text"/>	<input type="text"/>
R2 <input type="text"/>	R2 <input type="text"/>	<input type="text"/>
R3 <input type="text"/>	R3 <input type="text"/>	<input type="text"/>
R4 <input type="text"/>	R4 <input type="text"/>	<input type="text"/>
R5 <input type="text"/>	R5 <input type="text"/>	<input type="text"/>

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





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

Assessable Unit (AU) - Internal Control Assessment Summary										
Part 1: Assessable Unit Information										
<b>1. Assessable Unit Name:</b> <div style="background-color: #e6f2ff; height: 20px; width: 100%;"></div>										
<b>2. Assessable Unit Manager/Code:</b> <div style="background-color: #e6f2ff; height: 20px; width: 100%;"></div>										
<b>3. Assessable Unit Description:</b> <i>(The AU description should be clear, concise and written so anyone unfamiliar with the program/process will understand it.)</i> <div style="background-color: #e6f2ff; height: 20px; width: 100%;"></div>										
<b>4. Instructions/Guidance:</b> <i>(List all applicable directives/policies that govern the AU.)</i> <div style="background-color: #e6f2ff; height: 20px; width: 100%;"></div>										
<b>5. Assessable Unit Overall Risk Level:</b> <i>(From the AU Manager's Overall Risk Assessment rating on page 6 of the AU Risk Assessment Form, SEA 04Z 5200/1)</i> <div style="background-color: #e6f2ff; height: 20px; width: 100%;"></div>										
<b>6. Accomplishments:</b> <i>(Highlight area where you have become more effective or efficient, improved fiscal stewardship, or corrective actions have reduced Control Risk.)</i> <div style="background-color: #e6f2ff; height: 20px; width: 100%;"></div>										
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

## Enclosure 4 – Management Control Review Form

SUPSHIP MANAGEMENT CONTROL REVIEW FORM			
<b>1. ASSESSABLE UNIT (AU) TITLE:</b>			
<b>2. EVALUATION CONDUCTED BY:</b>			
a. NAME (Last, First, Code):		b. DATE OF EVALUATION:	
<b>3. IDENTIFY CONTROL BEING ASSESSED AND ASSOCIATED RISK(S):</b>			
a. CONTROL:		b. RISK(S):	
<input type="radio"/> AUTOMATED <input type="radio"/> MANUAL			
<b>4. IDENTIFY CONTROL TYPE (Check one):</b>			
PREVENTIVE <input type="radio"/>	DETECTIVE <input type="radio"/>	DIRECTIVE <input type="radio"/>	CORRECTIVE <input type="radio"/>
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
<b>5. METHOD OF TESTING KEY CONTROLS (Check all that apply):</b>			
a. DIRECT OBSERVATION <input type="checkbox"/>	b. FILE/DOCUMENTATION REVIEW <input type="checkbox"/>	c. ANALYSIS <input type="checkbox"/>	d. SAMPLING <input type="checkbox"/>
e. SIMULATION <input type="checkbox"/>	f. INTERVIEWS <input type="checkbox"/>	g. OTHER (Explain) <input type="checkbox"/>	
<b>6. ASSESSMENT RESULTS:</b>			
<i>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.)</i>			

**SUPSHIP MANAGEMENT CONTROL REVIEW FORM**

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

[Empty light blue box for internal control deficiencies]

**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).*

[Empty light blue box for corrective actions]

**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:

[Signature box for evaluator name]

b. EVALUATOR SIGNATURE:

[Signature box for evaluator signature]

c. AU MANAGER NAME AND CODE:

[Signature box for AU manager name and code]

d. AU MANAGER SIGNATURE:

[Signature box for AU manager signature]

## **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