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**, Management 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

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. 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**
			(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

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:

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:		
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				
						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:		
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					

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	
for the full risk verbiage see page 2	R2	
	R3	
	R4	
	R5	

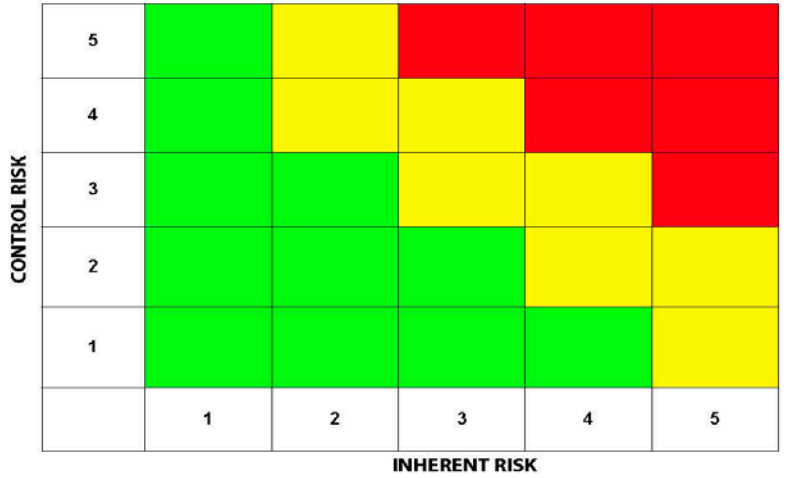
	INHERENT RISK	CONTROL RISK	COMBINED RISK
R1			
R2			
R3			
R4			
R5			

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

COMBINED RISK KEY

Low	Moderate	High

COMBINED RISK MATRIX



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