DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, D.C. 20350-3000

IN REPLY REFER TO:
2300-16A
IC4
25 Mar 22

From: Director, Information Command, Control, Communications, and Computers (IC4) Division, Deputy Commandant for Information (DC I)

Subj: INFORMATION RESOURCE MANAGEMENT (IRM) SEGREGATION OF DUTIES (SOD) ENTERPRISE POLICY

Ref: (a) DON IT Control Standards
(b) GAO-09-232G FISCAM
(c) OMB Circular A-130
(d) OMB Circular A-123
(e) ECSM 018 Marine Corps Assessment and Authorization Process
(f) ECSM 007 Resource Access Guide
(g) IRM 2300-21, USMC FSST and FSR Guidance

Encl: (1) IRM 2300-16A

1. Purpose. To provide direction for mitigating risks of inappropriate user access within and across financial and audit relevant systems, and to enable the prevention of such access. Where prevention is not possible, monitoring of user access to potentially unauthorized conflicting transactions and activities will be implemented through formal supervision, and review. This updates the existing Segregation of Duties (SOD) policy to strengthen business processes and information system access controls.

2. Cancellation. IRM 2300-16.

3. Authority. The information promulgated in this publication is based upon policy and guidance contained in references (a) through (g).

4. Applicability. This publication is applicable to contractors, Marine Corps Personnel, and Marine Corps Reserves who utilize and have oversight over Marine Corps information systems and connecting systems.

5. Scope.

a. Compliance. Compliance with the provisions of this publication is required unless a specific waiver is authorized.

b. Waivers. Waivers to the provisions of this publication will be authorized by the Director, Information Command, Control, Communications, and Computers (IC4) Division.

6. Sponsor. The sponsor of this technical publication is DCI-IC4-ICC-CIO.

L. A. DARKE
By direction

DIST STATEMENT A: Approved for public release; distribution is unlimited.
DISTRIBUTION: PCN 18652710900

MARINE CORPS INFORMATION RESOURCES MANAGEMENT (IRM)

2300-16A

SEGREGATION OF DUTIES (SOD) ENTERPRISE POLICY

March 25, 2022

Version 2.0

This page intentionally left blank

DOCUMENT CONFIGURATION CONTROL

The IRM Standards and Guidelines Program publications will be maintained at each receiving activity. Each activity is responsible for ensuring that their set of technical publications is complete, and that all published changes are promptly incorporated.

Version	Release Date	Summary of Changes
2300-16 V1.0	15 Apr 2020	Initial publication
2300-16A V2.0	25 Mar 2022	Major Revision / Reissuance

This page intentionally left blank

TABLE OF CONTENTS

This page intentionally left blank

EXECUTIVE SUMMARY

This Marine Corps manual provides guidance on the USMC’s Segregation of Duties (SOD) Enterprise Policy, and is published under the Marine Corps IRM guidance, which is based on the DON IT Control Standards as defined in reference (a).

This manual supports the Department of Defense (DoD) and Department of Navy (DON) directives, instructions, and policies governing Information Management (IM) and Information Technology (IT). The primary purpose of the SOD Enterprise Policy IRM is to promulgate detailed technical direction to the IM/IT communities in accordance with the Marine Corps Chief Information Officer’s (CIO) strategic vision and priorities. They are to be followed by Marine Corps commands, organizations, and detachments and provide a policy mechanism to communicate, coordinate, collaborate, and keep pace with Marine Corps Information Environment Enterprise (MCIEE).

This page intentionally left blank

SECTION 1.0: INTRODUCTION

1.1 Background

Marine Corps is modernizing their Enterprise environment in order to achieve auditability. This guidance is to reinforce existing standards, policies, and requirements and promulgate Segregation of Duties (sometimes referred to as "Separation of Duties") technical direction and compliance within the Marine Corps.

Segregation of Duties (SOD) can reduce the risk of a single individual having the capability to execute a particular task or set of tasks that are in conflict with each other. It is a preventive control that mitigates the risk of error and fraud in accounting and financial statements by requiring more than one person to complete a transaction-based task or activity. It is central to ensuring no employee or group is in a position to both perpetrate and conceal errors or fraud in the normal course of their duties without collusion.

The reference table below lists a few of the applicable policies.

Policy	Description	Applicability
A. Department of Navy (DON) Enterprise IT Control Standards.	This publication provides a customizable catalog of security and privacy controls for Department of Navy (DON) information systems addressing requirements across the US Navy and USMC and critical infrastructure.	The required control is Access Control (AC.5), Separation of Duties, which requires separation of organizational defined duties, documentation, and access enforcement. Related controls include AC.2, AC.3, and AC.6, which are further defined in Appendix A.
B. GAO-09-232G Federal Information System Controls Audit Manual (FISCAM).	This publication presents specific guidance for evaluating the confidentiality, integrity, and availability of information systems consistent with Generally Accepted Government Auditing Standards, also known as the Yellow Book and The Financial Audit Manual.	FISCAM is consistent with NIST guidelines and section 3.4 highlights the need for entity-wide SOD policies and procedures that are implemented at the system and application levels. Further, FISCAM guides evaluation around separation of work responsibilities so that one individual does not control all critical stages of a process.
C. Office of Management and Budget (OMB) Circular A-130, Responsibilities for Protecting and	This Circular establishes policy for the management of Federal information resources and applies to the information activities of all agencies of the	OMB A-130, Appendix I, section 4 (i) (3) establishes that each agency shall implement a policy of Separation of Duties to address the potential for abuse of authorized privileges and help to

Policy	Description	Applicability
cont. Managing Federal Information Resources.	**cont.** executive branch of the Federal government.	**cont.** reduce the risk of malicious activity without collusion.
D. OMB Circular A-123, Management’s Responsibility for Internal Control.	This Circular defines management's responsibility for internal control in Federal agencies. It also improves the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on internal control.	OMB A-123, section II (C) states that control activities include policies, procedures, and mechanisms to help ensure that agency objectives are met. Examples include proper segregation of duties (separate personnel with authority to authorize a transaction, process the transaction, and review the transaction); proper authorization; and appropriate documentation and access to that documentation.
E. ECSM 018 Marine Corps Assessment and Authorization Process.	This Manual provides techniques and procedures for the Assessment and Authorization (A&A) of systems and networks of the Marine Corps.	ECSM 018 provides guidance on the initial control baseline required for implementation.
F. ECSM 007 Resource Access Guide.	This Manual identifies a set of activities, general tasks, and structure to ensure secure Information Systems (IS) and IT operations, including the access and use of equipment, data, and user management of the Marine Corps Enterprise Network (MCEN).	ECSM 007, section 3.3 provides guidance regarding completing a System Access Authorization Request (SAAR).

1.2 Purpose

To provide direction for mitigating risks of inappropriate user access within and across financial and audit relevant systems, and to enable the prevention of such access. Where prevention is not possible, monitoring of user access to potentially unauthorized conflicting transactions and activities will be implemented through formal supervision, and review. This updates the existing Segregation of Duties (SOD) policy to strengthen business processes and information system access controls.

SECTION 2.0: ROLES AND RESPONSIBILITIES

2.1 Deputy Commandant for Information (DC I).

DC I will be responsible for:

a. Developing and overseeing Marine Corps policies and guidance for the implementation of the DON Enterprise IT Control Standards in accordance with (IAW) ref (a).
b. Performing compliance cross-application SOD analysis and reporting in support of Audit remediation efforts.
c. Maintaining an Enterprise repository of SOD matrices for in-scope systems.

2.2 Deputy Commandant for Manpower and Reserve Affairs (DC M&RA).

DC M&RA will be responsible for:

a. Tasking system owners for Marine On-Line (MOL), Marine Corps Total Force System (MCTFS), and subsystems (DTMS, MCPDT, MROWS, and UDMIPS) to provide user and role information to DC I for cross-application SOD analysis.
b. Providing a system point of contact authorized to provide user account and role information to the message POCs

2.3 Deputy Commandant for Installations and Logistics (DC I&L).

DC I&L will be responsible for:

a. Tasking system owners for Global Combat Support System – Marine Corps (GCSS-MC), Marine Ammunition Knowledge Enterprise (MAKE), and Internet Naval Facilities Assets Store (iNFADS) to provide user and role information
b. Providing a system point of contact authorized to provide user account and role information to the message POCs

2.4 Deputy Commandant for Programs and Resources (DC P&R).

DC P&R will be responsible for:

a. Tasking system owners for Defense Agencies Initiative (DAI) to provide user and role information.
b. Providing a system point of contact authorized to provide user account and role information to the message POCs.
c. Providing business risk input from the applicable IT system business-side offices to the System Owners in conjunction with the System Owners implementing cross-application SOD controls associated with Marine Corps Financially Significant and Sensitive Transactions (FSST) and Financially Significant Resources (FSR) systems.

2.5 System Owners.

System Owners with guidance from DC I, and in conjunction with Key Financial Stakeholders will be responsible for evaluating the relevant End-to-End business process and IT roles for their information systems to identify roles, responsibilities and accesses that could be segregated so that one individual does not control all critical stages of a process. Additionally, System Owners have responsibility for system-level governance over SOD processes associated with their specific Marine Corps FSST system(s), activities, and resources. This includes implementing cross-application SOD controls associated with the Marine Corps FSST and FSR systems. System Owners, in conjunction with P&R have responsibility for developing SOD matrices for their specific systems, and storing them in the IC4 Enterprise repository (Appendix D).

2.6 Key Financial Stakeholders.

Key Financial Stakeholders (Appendix B) will be responsible for coordinating with the System Owners in evaluating the relevant End-to-End business process and IT roles for their information systems to identify roles, responsibilities and accesses that could be segregated so that one individual does not control all critical stages of a process.

SECTION 3.0: SOD ENTERPRISE POLICY

Effective segregation of duties are implemented at the system, application level and across applications. Therefore, the IT Enterprise, System Owners and Key Financial Stakeholders (Key Financial Stakeholders are identified in Appendix B) must:

(1) Evaluate the relevant End-to-End business process and Information Technology (IT) roles for their information systems,

(2) Identify combinations of incompatible roles that could allow a user to subvert segregation of duties (such as through perpetration and concealment of unauthorized transactions or system activities),

(3) Design control requirements and document control implementations to prevent users from performing incompatible duties,

(4) Assess the risk where SOD is not feasible and establish compensating controls, and

(5) Require written authorizations, (e.g., waivers) for segregation of duties conflicts prior to granting access to transactions or activities in their area of responsibility and associated compensating controls implemented for monitoring of the conflict. However, all waivers must be conditional on the periodic monitoring of the waived user’s system activity. Waivers without an associated compensating monitoring control are not an effective alternative.

The System Owners and Key Financial Stakeholders have responsibility for system-level governance over SOD processes associated with their specific Marine Corps FSST system(s), activities, and resources. Additionally, the System Owners are responsible for implementing cross-application SOD controls associated with Marine Corps financially significant sensitive transactions (FSST) and Financially Significant Resources (FSR) systems, in conjunction with business risk input from the applicable IT system business-side offices, including Programs and Resources. Specifically, Segregation of Duty (SOD) matrices list incompatible procedures/functions and overarching processes the system supports. Procedures and functions that are incompatible with others may indicate financially significant sensitive transactions that are performed within them. For detailed requirements for the FSST and FSR areas, refer to IRM 2300-21, USMC Financially Significant Sensitive Transactions (FSST) and Financially Significant Resources (FSR) Guidance, dated March 18, 2022.

The sections below provide the requirements and examples for identification, documentation, and enforcement of this SOD policy. The lists should not be considered complete as other requirements or tailoring may be necessary for a given process or environment.

Additional policies and processes will be established and distributed to support the Marine Corps implementation of SOD.

3.1 Evaluation and Identification

System Owners and Key Financial Stakeholders must evaluate the relevant End-to-End business process and IT roles for their information systems to identify roles, responsibilities and accesses that could be segregated so that one individual does not control all critical stages of a process. An assessment process shall be performed to identify and evaluate the below risk areas:

- **System support functions** such as information security management, systems design, applications programming, systems programming, quality assurance and testing, library management/change management, computer operations, production control and scheduling, data security, data administration, network administration, and configuration management.
- **Functional roles and responsibilities** for each Marine Corps mission area, functional area, program area and other organizational units involved in a process, including business and information system processing roles and responsibilities not identified above. The OUSD End-to-End Business Processes may be utilized to identify these areas.
- **Sensitive and high-risk** transactions and processes across financial and operational areas such as authorizing, processing, recording, and reviewing key financial transactions.
- **Exceptions** such as roles allowed for emergency and temporary authorizations. These are typically exceptions to the rules.
- **Manual processes** and **system automation** that can lead to violations in SOD.
- **Non-person activities** that do not require human interaction, but requires privileged access in order to perform the expected tasks, such as service accounts, system accounts, devices, software, enterprise applications incorporated modules, etc.
- **Other roles** such as those assigned to all users that when joined with existing access or roles assigned through mobile devices that could create a violation in SOD.

System Owners and Key Financial Stakeholders should ensure that SOD principles are established, enforced, and institutionalized within their area of responsibility through physical and logical access controls.

3.2 Documentation

All SOD restrictions and elements (systems, applications, processes, entities, groups, locations, roles, duties, boundaries, etc.) should be identified and clearly defined in all documents. For example, incompatible duties should be identified for each system and embedded in related system documentation, such as:

- **System Security Plan**. This document contains related NIST SP 800-53 controls, to include AC-5 Separation of Duties and related controls to be implemented and appropriately tailored. References to NIST SP 800-53 controls must consider the requirements of DON Enterprise IT Control Standards and align to the more restrictive requirement (see Appendix A);

  - AC-3 Access Enforcement
  - AC-6 Least privileged
  - AU-2 Audit Events
  - AU-6 Audit Review, Analysis, and Reporting
  - PE-3 Physical Access
  - PE-4 Access Control of Transmission Medium
  - PS-2 Position Risk Designation

- **SOD Diagram and/or Matrix**. This document depicts the processes to be used as the basis to build and maintain the SOD environment, and to check for incompatibilities before granting access.

- **Interface Control Agreements (ICAs)/ Memorandums of Understanding (MOUs) / Memorandum of Agreements (MOAs)**. This document establishes formal agreements between connecting systems.

- **System Authorization Access Request (SAAR)**. This document defines the assigned roles and allows formal approval for new and changed user accounts. For example, privileged user accounts should only be used for those activities as spelled out in the SAAR. Privileged users shall have separate accounts for day-to-day operations that have been evaluated against SOD for both accounts, and that are monitored for noncompliance, as well as unusual activity.

3.3 Enforcement

SOD is implemented through a combination of manual and automated access controls to restrict access to resources, processes, and systems. Only those users specified by the System Owners may have some combination of read, write, execute, and/or other permissions to an application or system as defined in the SOD Matrix for that system and authorized in the respective SAAR. For example, the same user should not be able to create a vendor and post a payment to the same vendor. Identifying and defining duties that should be separated is an important control activity that helps prevent errors and/or improper activities. The below categories of duties or responsibilities, although not all encompassing, are considered incompatible and must be separated.

Where possible, the systems should be configured to create segregation between:

- System Support Functions and Functional Roles.
- Administrator roles that implement information system controls and roles that approve configuration and verify changes.

- Security personnel roles that administer access control functions and roles that can execute audit logging / monitoring functions.
- Developer roles that can develop key report queries and roles that approve the logic and accuracy of those queries.
- Personnel roles that update vendor/employee records and roles that approve financial transactions
- Personnel roles that process transactions and roles that authorize access to systems/applications.
- Personnel roles initiating a transaction and roles that approve the same transaction.
- Non-privileged user roles and roles that can execute privileged functions to include disabling, circumventing, or altering security measures.

Additional examples of segregations to be enforced can be found in DON Enterprise IT Control Standard AC.5.a found in Appendix A.

Privileged roles (both IT and financial) should be identified and limited to the minimum acceptable number of personnel necessary to carry out the duties associated with the role of a privileged user. Because of the nature of today’s operational environment, it is understood that segregation of duties alone will not ensure that personnel perform only authorized activities; therefore, additional controls are to be identified and implemented to prevent or detect incompatible permissions and/or actions.

For those systems owned by non-Marine Corps entities, the System Owners and Key Financial Stakeholders must be able to produce documentation that verifies compliance to SOD policy for all externally connected systems.

3.4 Exceptions

Information systems with few users often find it impossible to fully implement SOD due to limited personnel for which duties can be assigned. In these instances, it is necessary for the System Owners and Key Financial Stakeholders to establish mitigating controls, which must be documented and implemented in accordance existing standards, policies and requirements. In order to be adequate, those mitigating controls should be designed to either prevent, or detect through system activity monitoring, unauthorized actions that could result from permitting incompatible combinations of roles. In these situations, direct leadership involvement provides a strong deterrent to conflicting activities.

This page intentionally left blank

Appendix A: DON IT Control Standards for SOD-Related Controls & Artifacts

Segregation of Duties activities highlighted in the SOD guidance are consistent with the DON IT Control Standards, NIST SP 800-53, CNSSI No. 1253, and OMB information security control-related policies and guidance. The below chart highlights the SOD related controls, to be included and tailored, as required.

Standard Number	DON Enterprise IT Control Standards for Access Control (AC)	FISCAM Control Objective	Evidence	Evidence Frequency
AC.2.a	**Establishing and Activating User Access** System Owners must implement a process that users' access requests are approved based on the following criteria: • User access requests have been endorsed/signed by the user's supervisor as necessary for the user's job functions. • A standard access request form must be used and include, at a minimum the following information: □ User identification information; □ Type(s) of access required; and □ Justification for access, □ Types of access, privileges, roles, and groups requested, and; □ Verified completion of information/security awareness (IA) training requirements. • ISSM or ISSO when approving access requests shall employ the concept of least privilege, and not approve more access than is necessary for users to perform their jobs. • ISSM or ISSO when approving access requests shall employ the	AC-3	Access Control Policy and Procedures document(s). Completed User Access Approval Forms for the current fiscal year. System generated listing of user accounts showing the level of access (e.g., roles, privileges) within the system.	Annually Per Instance as Required Per Instance as Required

Standard Number	DON Enterprise IT Control Standards for Access Control (AC)	FISCAM Control Objective	Evidence	Evidence Frequency
	cont. concept of separation of duties, so that user access or privileges are not granted for incompatible duties, i.e. duties which if assigned together would increase the potential for malevolent activity or abuse of privileges. • The O/S, DB, and Application shall enforce separation of duties automatically via access and privileges restrictions. If manual, the System Owner shall compare requested access to a separation of duties matrix prior to provisioning access to ensure that incompatible duties will not be assigned. System Owners shall ensure a process to maintain an audit trail of approved access.			
AC.2.b	**Reviewing User Access** System Owners shall ensure each account's access permissions, and their specific levels of access, are reviewed annually, at a minimum, by an independent reviewer, who has knowledge of the user's job responsibilities to determine whether the access is still required (i.e., if need-to-know changes). Additionally, System Owners shall ensure that the following reviews, are performed at a minimum for accounts at the O/S, DB, and application layers (or more stringent as required by applicable Navy policy): 1. Annual review of the separation of duties matrix or separation of duties assessment that identifies incompatible user access; 2. Annual review of authorized user accounts and access at the OS, DB, & application layers for continued need	AC-3	Access Control Policy and Procedures document. Review of the separation of duties matrix or separation of duties assessment that identifies incompatible user access. Review of privileged accounts and their access. Review of unnecessary accounts (default, guest, etc.). User accounts have been reviewed (e.g., emails, reports, and	Annually Annually Quarterly Quarterly Annually

Standard Number	DON Enterprise IT Control Standards for Access Control (AC)	FISCAM Control Objective	Evidence	Evidence Frequency
	cont. and appropriateness; 3. Quarterly review of privileged accounts and access at the OS, DB, & application layers for continued need and appropriateness; and 4. Quarterly review for unnecessary accounts (e.g., default, guest, etc.). For further guidance regarding access reviews, refer to the FMP Process Guidance For User Access Review (UAR).		**cont.** other evidence of these reviews) to include username, roles and date of review within the current fiscal year.	
			Evidence of independent reviewer's appropriateness (e.g. organizational chart or human resources listing).	Annually
			System generated listing of user accounts showing access roles & privileges in the system	Per Instance as Required
AC.2.c	**Modifying and Disabling** If the individual's access is required to be changed as a result of the review identified in control AC.2.b, System Owners shall ensure System Administrator(s) modify or disable the user's access. For access that is expired or is no longer supported by a business justification, System Owners shall ensure System Administrator(s) disable or remove the account within 72 hours upon notification. Disabled accounts can be either archived or removed.	AC-3	Access Control Policy and Procedures document.	Annually
			System generated listing of user accounts showing account status and date/time of last user access that documents the date that each account (as applicable) is disabled or modified.	Per Instance as Required

Standard Number	DON Enterprise IT Control Standards for Access Control (AC)	FISCAM Control Objective	Evidence	Evidence Frequency
			cont. System generated listing of user accounts showing access roles & privileges in the system	Per Instance as Required
AC.2 (1)	**Control enhancement: 1** *ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT* The System Owner shall ensure the system is configured to employ automated mechanisms to support the information system account management functions.	AC-3	Access Control Policy and Procedures document. System generated evidence that demonstrates configuration settings are established for automatic mechanisms to support system account management functions.	Annually Per Instance as Required
AC.3.a	System Owners shall ensure that the nature and extent of access available to each user to a given resource (OS, DB, and Application) is no more access than necessary for each user to perform their job functions. Individuals shall only be granted access based off of a valid business purpose (least privilege). On an annual basis, System Owners shall ensure that a review of all access rights assigned for all accounts is performed for validation of continued appropriateness.	AC-3	Access Control Policy and Procedures document. Evidence that access rights assigned to accounts have been reviewed for appropriateness (e.g., emails, reports, and other evidence of these reviews) to ensure that each user is only granted access that is	Annually Annually

Standard Number	DON Enterprise IT Control Standards for Access Control (AC)	FISCAM Control Objective	Evidence	Evidence Frequency
			cont. necessary based off of a valid business purpose.	
AC.3.b	System Owners shall maintain proper control of information system processes and services to ensure the confidentiality, integrity, and availability of user data in cognizance of the risks detailed in the Risk Assessment Report (RAR).	AC-3	Access Control Policy and Procedures document. Risk Assessment Report	Annually Per Instance as Required
AC.5.a	System Owners shall define and document separation of duties and incompatible functions and implement the following principles: • Application users shall not have access to operating systems or applications software; • Programmers shall not be responsible for moving programs into production or have access to production libraries or data; • Access to operating system documentation shall be restricted to authorized systems programming personnel; • Access to applications system documentation shall be restricted to authorized applications programming personnel; • Access to production software libraries shall be restricted to library management personnel; • Persons other than computer operators shall not set up or operate the production computer; • Only application users, not system administrator, shall be responsible for transaction origination or correction and for initiating changes to application files; and • Computer operators shall not have access to program libraries or data files.	SD-1	Access Control Policy and Procedures document. Documented evidence of review of the Separation of Duties Matrix.	Annually Annually

Standard Number	DON Enterprise IT Control Standards for Access Control (AC)	FISCAM Control Objective	Evidence	Evidence Frequency
	cont. Organizations with limited resources to separate duties shall implement compensating controls to mitigate risks of conflicts in separation of duties. These compensating controls shall be documented in the Access Control Policy and Security Plan.		**cont.** SoD waivers for user accounts with conflicting access.	Per Instance as Required
	For further guidance regarding access reviews, refer to the FMP Process Guidance For User Access Review (UAR)		System generated listing of user accounts and their access roles & privileges	Per Instance as Required
AC.5.b	System Owners shall define and document a separation of duties matrix (matrices) which includes roles (both from functional and/or system perspectives) & privileges. The matrix shall list all roles and responsibilities that exist, and identify any combination of roles and responsibilities that shall not be granted together to a user, based on their duty functions and least privilege.	SD-1	Access Control Policy and Procedures document.	Annually
	System Owners shall ensure an annual review is performed of the separation of duties matrix to ensure that the current operating environment is reflected.		Evidence of annual review of separation of duties matrix to include all changes that were made and the date of the change and individual that made the change.	Annually
AC.5.c	System Owners shall define and document how transaction processing is utilized in the operating environment and identify any incompatible transaction processing functions or combinations of functions that shall not be performed by a single individual, such as: • Data entry and verification of data;	SD-1	Access Control Policy and Procedures document.	Annually

Standard Number	DON Enterprise IT Control Standards for Access Control (AC)	FISCAM Control Objective	Evidence	Evidence Frequency
	cont. • Data entry and its reconciliation to output; • Input of transactions for incompatible processing functions (for example, input of vendor invoices and purchasing and receiving information); and • Data entry and supervisory authorization functions (for example, authorizing a rejected transaction to continue processing that exceeds some limit requiring a supervisor's review and approval).			
AC.5.d	System Owners shall ensure that documented job descriptions exist and clearly describe employee duties as well as prohibited activities that could cause separation of duties conflicts within the organization. These shall include responsibilities that may be assumed during emergency situations. Resources and training shall be provided to educate employees of their responsibilities to ensure that separation-of-duties principles are established, enforced, and institutionalized within the organization. Job descriptions shall be documented for all roles within the organization.	SD-1	Access Control Policy and Procedures document. Security awareness training to included education regarding separation-of-duties principles. Documented job descriptions that describes employee duties	Annually Annually Annually
AC.6.a	System Owners shall identify individuals with access to sensitive financial/functional roles, sensitive system resources and the business purpose (i.e. based on the user's job responsibilities, the access shall be commensurate with that role) for this access. System Owners shall ensure the number of individuals with access to services and processes shall be restricted based on the concept of least privilege (the least amount of	AC-3	Access Control Policy and Procedures document. System generated configuration settings denoting automatic removal **cont.** or disabling of temporary accounts after 72 hours.	Annually Per Instance as Required

Standard Number	DON Enterprise IT Control Standards for Access Control (AC)	FISCAM Control Objective	Evidence	Evidence Frequency
	cont. access necessary for user to perform their job) that is appropriate for their environment. Unnecessary accounts (default, guest accounts) are removed, disabled or otherwise secured at the O/S, DB, and Application level. For more information regarding reviewing accounts based on the concept of least privilege. See AC.5.a, AC.5.b, AC.5.c, and AC.5.d – Separation of Duties, for additional guidance. For further guidance, refer to the FMP Process Guidance for Financially Significant Sensitive Transactions		Review of information system accounts for compliance with account management requirements. Analysis which lists identified financial/functional significant sensitive transactions and resources.	Annually Per Instance as Required
AC.6(1)	"Control enhancement: 1 LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS " System Owners shall ensure that access to all security functions (deployed in hardware, software, and firmware) and security-relevant information that are not publicly accessible are explicitly authorized. Access Control Policy and the related implementation procedures shall document how the concept of least privilege is employed, allowing only authorized accesses for user (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions, and includes the following requirements: • Limiting privileged accounts, including super user accounts, to a small number of personnel;		Access Control Policy and Procedures document. Evidence of appropriate approval by upper management in a corresponding access authorization form for all users.	Annually Annually

Standard Number	DON Enterprise IT Control Standards for Access Control (AC)	FISCAM Control Objective	Evidence	Evidence Frequency
	cont. • Denying access unless specifically authorized and approved based on assigned job duties; • Denying access unless explicitly authorized and allowed such as privileged and deployed hardware, software, firmware, and to security functions and information, and networks/remote access; • Denying access to non-security functions through a privileged security account or role; • Restricting access to only allowable, approved commands; and • Denying non-privileged users from executing privileged security functions such as disabling, circumventing, or altering security functionality.			
AC.6(2)	"Control enhancement: 2 LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS" System Owners shall ensure that users of system accounts, or roles, with access to any privileged security functions or security-relevant information, use non-privileged accounts or roles, when accessing non-security functions.	AC-3	Access Control Policy and Procedures document.	Annually
AC.6(5)	"Control enhancement: 5 LEAST PRIVILEGE | PRIVILEGED ACCOUNTS" System Owners shall define and document the personnel or roles to whom privileged accounts (e.g., system administrator) are to be restricted on the system and implement a process to only provide privileged accounts on the information system to the defined personnel or roles.	AC-3	Access Control Policy and Procedures document. Evidence of system generated configuration settings demonstrating only authorized personnel or roles have access to privileged accounts.	Annually Per Instance as Required

Standard Number	DON Enterprise IT Control Standards for Access Control (AC)	FISCAM Control Objective	Evidence	Evidence Frequency
AC.6(9)	"Control enhancement: 9 LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS " System Owners shall ensure that the given system is configured to audit the execution of privileged functions.	AC-3	Access Control Policy and Procedures. Evidence of system generated configuration settings demonstrating auditable events tracking privileged user activity.	Annually Per Instance as Required
AC.6(10)	"Control enhancement: 10 LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS" System Owners shall ensure that system is configured to prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. Examples of privileged functions include establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities.	AC-3	Access Control Policy and Procedures document. Evidence of system generated configuration setting (e.g., screenshot) prohibiting non-privileged users from executing privileged functions.	Annually Per Instance as Required

This page intentionally left blank

Appendix B: Financial Oversight Stakeholder Organization by Business Process

The Table below identifies the respective processes and identifies key financial stakeholders. System Stakeholders should obtain approval from key financial stakeholders in the identification of financially significant sensitive transactions/resources and provide a financial oversight approval.

Financial Oversight Stakeholder Organization by Business Process	
Business Process	Key USMC Financial Stakeholders
Transportation of People	DC I&L
Civilian Pay	DC M&RA
Civilian Permanent Change of Station (PCS)	DC M&RA
Military Pay	DC M&RA
Military Permanent Change of Station (PCS)	DC M&RA
Contractor Vendor Pay	DC I&L/MCSC DC P&R
Fund Balance with Treasury	DC P&R
Financial Statement Compilation and Reporting	DC P&R
Fund Receipt and Distribution	DC P&R
Reimbursable Work Orders-Grantor and Performer	DC P&R
Transportation of Things	DC I&L
Operating Material and Supply	DC I&L/MCSC
Real Property	DC I&L/MCICOM
Military Standard Requisitioning and Issue Procedures	DC I&L/LOGCOM
USMC Inventory	DC I&L/LOGCOM
General Equipment	DC I&L
Collections and Disbursements	DC P&R
Revenue Rate Setting	DC P&R
Contingent Legal Liabilities	CMC Counsel
Environmental Disposal Liabilities	DC I&L - Equipment DC I&L - Real Property

This page intentionally left blank

Appendix C: Glossary

Acronym	Defined
AC	Access Control
AU	Audit and Accountability
C4	Command, Control, Communications, and Computers
CIO	Chief Information Officer
CM	Configuration Management
CNSSI	Committee on National Security Systems Instruction
DC I	Deputy Commandant for Information
ECSM	Enterprise Cybersecurity Manuals
FISCAM	Federal Information System Controls Audit Manual
FSR	Financially Significant Resources
FSST	Financially Significant Sensitive Transactions
GAO	Government Accountability Office
HQMC	Headquarters Marine Corps
IC4	Information Command, Control, Communications, and Computers
ICA	Interface Control Agreement
ICC	Information C4 Compliance Branch
IRM	Information Resource Management
IS	Information System
ISSM	Information Systems Security Manager
ISSO	Information System Security Officer
IT	Information Technology
MCCOG	Marine Corps Cyberspace Operations Group
MCEN	Marine Corps Enterprise Network
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PM	Program Management`
PS	Personnel Security
RAR	Risk Assessment Report
SAAR	System Authorization Access Request
SI	System and Information Integrity
SLA	Service Level Agreement
SOD	Segregation/Separation of Duties
SP	Special Publication
USMC	United States Marine Corps

This page intentionally left blank

Appendix D: In-Scope Systems' SOD Matrices and Conflict Schedules

The following In-Scope Systems' SOD Matrices and Conflict Schedules are located at: https://usmc.sharepoint-mil.us/:f:/r/sites/DCI_IC4_Audits/Audits%20Documents/SOD?csf=1&web=1&e=UUguD7

For in-scope System Owners that are currently remediating IPA-noted SOD matrix weaknesses, please post your updated SOD matrices to this restricted access site, once approved.

- DAI-ERP.
- GCSS-MC (Note 1).
- iNFADS.
- MAKE.
- MCTFS.
- MOL-DTMS.
- MOL-MCPDT.
- MOL-MROWS.
- MOL-UDMIPS (Note2.

Notes:

1. CAP milestone date to complete GCSS-MC SOD Matrix: June 30, 2022.
2. On 3-17-22 a draft UDMIPS SOD matrix was developed by IC4's contract support team. On 3-21-22 Mr. Darrell P. Jansen, MISSA Integrated Applications, MANDR AFFAIRS, emailed his concurrence with the accuracy of the UDMIPS SOD matrix, which is now included in the SharePoint repository identified above.

This page intentionally left blank. Last page of IRM.