CONTENT: This instruction describes roles and responsibilities required to maintain an effective Segregation of Duties (SoD) environment in Saudi Aramco SAP implementations.

This GI covers the following scope: The detection, remediation and prevention of SoD violations for users of corporate SAP processes where financial information is processed. All Finance owned processes are within this scope, and non Finance owned processes which have significant financial impact are considered also.

The text of this GI includes:

1. GLOSSARY

AP&SD	Accounting Policies & Systems Department.
SoD System	The SoD system is the software used in Saudi Aramco to build the database of Segregation of Duties rules and to run the detection and monitoring reports to identify potential SoD violations in existing SAP implementations.
SoD Analysis	After an extract of authorization data has been completed but before SoD violation reports can be run an SoD analysis must be run. This analysis summarizes the extract data into tables that facilitate the generation of SoD violation reports.
SoD Extract	On a scheduled basis the SoD software extracts all SAP authorization data from a specified SAP system, e.g. PRC. This authorization data is used for analyzing SAP authorizations against SoD rules.
CAD	Computer Applications Department
Compensating Controls	In the case of an SoD violation, a Proponent Organization or an End User organization may identify the existence of manual or system controls that allow the user to continue to have the existing authorizations, as this control mitigates the risk associated with the violation. Proposed compensating controls should be approved by AP&SD before implementation in the SoD database. Compensating Controls can be applied to user assignment violations only.
DPSR	Data Processing Service Request.
EDPD	Enterprise Data Protection Division.
End User Organization	For Segregation of Duties, the End User organization refers to organizations that request user assignments to SAP roles that are owned by Proponent Organizations. End User organizations are responsible to remediate any existing SoD violations in their organizations. They will also participate in developing and reviewing the SoD rules and

	Compensating Controls.
HAD	Hydrocarbon Applications Department
Mitigation	Mitigation refers to the process of assigning compensating controls to violations.
Proponent Organization	For Segregation of Duties, the Proponent Organization refers to the **Data Owner** of the SAP roles within a particular SAP system, for example AP&SD is the Data Owner of all Finance roles in PRC, PRH and PRO. Proponents are responsible for developing and maintaining SoD Rules relating to financial processes in SAP. This should be done in consultation with End User organizations and Subject Matter Experts for a particular business cycle.
Remediation	Remediation refers to the process of fixing reported violations by taking one or more of the following actions: • Revoking a user's access to a role. • Fixing a violating role by changing the transactions or authorizations within the role that cause the role to be in violation of a rule. • Adding a compensating control to the rulebook and applying the control to the specific violation. This process is often referred to as mitigation. • Altering the SoD rule which caused the violation to exist. This can only be done if the rulebook owners and AP&SD Subject Matter Experts (SME's) are in agreement that the rule needs to be refined.
Remediation Tool	In support of Saudi Aramco SoD, a program has been developed to assist End Users in the effort of maintaining the actions that they plan to take to clear the SoD violations that exist in their organization. This program is often referred to as the remediation tool.
SAP Roles	An SAP role is a group of SAP transactions with authorization objects and values, which together enables the full access rights to complete the defined transactions.
SoD Rulebook	A rule book is a collection of SoD rules. Rulebooks are organized into the following business cycles: Requisition to Payment (R2P), Order to Cash – Export Sales (O2CE), Order to Cash – Local Sales (O2CL), Hire to Retire (H2R), Build to Dispose (B2D), Record to Report (R2R) and Treasury (TR).
SoD Rules	SoD Rules in the SoD system are the basis on which SoD control is built. An SoD rule identifies two groups of transactions and authorizations that should never be assigned to the same user. These transaction groups should not be implemented in one SAP role, nor should be assigned to a user through two or more roles. These transaction and authorization groups must be segregated. Giving a user access to these transactions

	will create an SoD violation. Accurately defining the SoD Rules for a particular business cycle enhances the quality of all subsequent steps in the SoD process.
SoD Violation	An SoD violation is a conflict in granted authorizations in SAP. The conflict is identified by the SoD system based on the SoD Rulebooks. There are two types of violations: 1) **Role Violations** which means that there is a combination of transactions and authorizations within the role that must be segregated. 2) **User Assignment Violations** which identifies a conflict in the authorizations that a user is assigned in two or more roles.
SSAD	Support Services Applications Department
UAMT	User Access Management Tool. UAMT is the corporate user provisioning tool used to manage assignment of users to SAP roles.
User Assignments	User assignment refers assignment of SAP Roles to users in order for them to perform specific functions within SAP.
What-If Analysis	What-If Analysis is a feature of the SoD database system that allows SoD users to simulate and report the potential SoD risks associated with a new user role assignment or a role modification. For SoD prevention, What-If Analysis must be run against all role modifications before a role can be transported to production.

2. OVERVIEW

2.1 Fundamental Principles. A fundamental principle of internal control is that sensitive functions, which are potentially harmful to the corporate interest, should be segregated so that no one person controls all aspects of that function. Segregation of Duties is desirable to prevent fraudulent transactions; to preserve data integrity that will ensure accurate reporting and the timely detection of errors; and to prevent unintentional actions beyond the scope of what is authorized and approved by management.

The four general categories of duties or responsibilities which should be segregated are:

Record keeping: Creating and maintaining records – within this category master data is typically segregated from transactional data.
Custody: Access to and/or control over physical assets.
Authorization: Reviewing and approving transactions.
Reconciliation: Assurance that transactions are accurate, valid and proper.

2.2 SoD Rule and Rulebook Development. A framework of SoD Rules and Rule Books has been developed by cross functional teams from Proponent and End User organizations and Subject Matter Experts from AP&SD. These Rule Books have been deployed, and approved by the Proponent Organization, for the high risk financial processes of the following Business Cycles in the Saudi Aramco SAP Production environments:

1. Hire To Retire (H2R)
2. Order to cash for local sales (O2C-L)
3. Order to cash for export sales (O2C-E)

4. Requisition To Payment (R2P)
5. Build To Dispose (B2D)
6. Treasury
7. Record to Report (R2R)

2.3 Ongoing SoD Remediation. The SoD Rules are analyzed against SAP Authorization data to detect existing SoD violations in SAP Roles and SAP User Role Assignments. Violations are remediated either by assigning compensating controls, making role changes or revoking user access to one or more roles.

2.4 Ongoing Prevention of SoD Violations. The introduction of new SoD violations must be prevented during the user provisioning process, during Role maintenance and system developments. The SoD Rules and Rule Books have been integrated into the User Access Management Tool (UAMT), to detect potential SoD violations before SAP Roles are assigned to users .

3. STANDARDS AND GUIDELINES

3.1 BUSINESS PROCESS ANALYSIS

3.1.1 Systems Development Life Cycle: Segregation of Duties concepts must be reflected during all phases of the system development life cycle:

3.1.1.1 Where a financial business process is developed, extended or enhanced, the new or modified process steps need to be analyzed to identify potential SoD Risks.

3.1.1.2 All new programs and changes to existing programs need to be analyzed to determine whether they constitute any SoD risks.

3.1.1.3 Details of all evaluation and analysis results (SAP roles, transactions, authorization objects and values) must be documented in the relevant systems development documentation such as the DPSR, High Level Design Document or Low Level Design Document.

3.1.1.4 Program test scripts for Unit Testing, Integration Testing and User Acceptance Testing must include reference to SoD analysis and testing and signed off by the Proponent Organization.

3.1.1.15 No SAP roles may be transported to production systems that may introduce new SoD risks or violations.

3.1.2 Continuous Evaluation: Based on a business process risk assessment, the initial scope of SoD was limited to the high risk business processes. It is now the responsibility of the proponent organization to extend the analysis to their lower risk processes as well, and of the End User organizations to follow through with any subsequent remediation work based on these analyses.

3.1.2.1 Regular reviews of SoD violation reports must be established by proponents and violations must be communicated to end user organizations for their action.

3.1.2.2 Proponent organizations must analyze, evaluate and document any additional SoD Risks that were not included in the initial scope of SoD.

3.2 RULEBOOK MANAGEMENT

3.2.1 Rulebook Ownership: Each of the SoD Rule Books in the SoD database is owned by a Proponent Organization that is responsible for maintaining the content of the rules in the SoD Development system.

3.2.2 Rulebook Changes: Changes to Rule Books must be approved by the Rule Book Owner and concurred by AP&SD before any changes are made. Only approved and concurred Rule Change Request Forms will be accepted by Enterprise Data Protection Division (EDPD) to transport rule books across the SoD landscape.

3.3 AUTHORIZATION DATA

The SAP authorization data which is used for generating SoD analyses and violation reports must be kept current in the SoD system to ensure the accuracy of reports.

3.4 SoD VIOLATION REPORTS

The SoD database management system generates standard reports of user and role violations. All proponents are responsible to generate and review violation reports and to communicate them to impacted organizations for the necessary remedial actions to mitigate or eliminate SoD violations.

3.5 REMEDIATION

SoD Violations can be remediated by (i) revoking access; (ii) redesigning SAP Roles; (iii) assigning compensating controls that may mitigate or eliminate the SoD Risk (iv) modifying the rule which generated the violation. These actions, as well as target dates for implementation, must be recorded in the Remediation Plan.

3.5.1 Remediation Plan: Each organization with SoD violations must record their remediation actions and implementation dates in the remediation plan. An automated *Remediation Tool* has been developed and interfaces with the SoD database to record the actions required against all SoD Violations.

3.5.2 Revoke Access: Where users are violating an SoD Rule their access must be revoked from the conflicting roles if no compensating controls are available and if the role is not being redesigned.

3.5.3 Redesign Roles: Where SoD conflicts exist within the role, the role needs to be redesigned to remove the conflicting transactions. The 'what-if analysis' must be applied to prevent any SoD conflicts being allowed in the role. Established role change procedures for the design, testing, approval and transport must be followed. Once the role(s) are reassigned to users, prevention procedures must be applied to prevent user SoD violations.

3.5.4 Compensating controls: A Proponent Organization may assign a compensating control if it is not possible to revoke the user's access or redesign and reassign the role to achieve SoD. Compensating controls are subject to the following conditions:

3.5.4.1 Compensating controls must be documented and tested by the Rule Book owner and approved by AP&SD before it can be implemented in the SoD production system.

3.5.4.2 Compensating controls must have an expiry date when they are created, and not for more than one year from the creation date.

3.5.4.3 A compensating control may be assigned to a specific user by his department manager and will allow the user to use conflicting roles until the compensating control expiry date has been reached or until the expiry of the role assignment date as specified by the department manager; whichever is the earlier date.

3.5.4.4 Before the compensating control expires, it must be reviewed, tested and recertified by the Proponent Organization before a new expiry date can be set.

3.5.5 Rule Book Changes: A Proponent Organization may change a Rule or a Rule Book in the SoD database based on observations from End User organizations, SME's or Internal Auditing. Rule Book changes must be approved by AP&SD.

Internal Auditing may review and test any compensating controls for accuracy, completeness and validity during audit reviews.

3.6 PREVENTION

3.6.1 User Assignment Violations: The user provisioning process (SAP Role assignment requests) has been automated through the UAMT. The SoD Rulebooks have been incorporated with the UAMT to automatically detect whether a role assignment request will create an SoD violation. If no violation is detected the role assignment will proceed normally. However, if violations are detected, requests will be handled in the following manner:

3.6.1.1 If a violation is detected and no compensating control exists for this violation, the request will be rejected.

3.6.1.2 If a compensating control exists for the violation, the Rule Book owner must decide whether to apply this control to the specific SoD violation.

3.6.1.3 Where UAMT is not used for role assignments, such as direct assignments with SAP tools like the Profile Generator or User Master Maintenance screens, controls must be in place to ensure that (usually on an emergency basis) role assignments are subject to SoD reviews. Position based role assignments made through HR must also be subject to SoD controls.

(See the Appendix on User Assignments for more details).

3.6.2 Role Violations: If a role change or role creation request is initiated EDPD must first ensure that the new or modified role is analyzed with the SoD system 'What-if' functionality. This

will detect whether the role will create violations when transported to production. Only roles that are violation free can be transported to production.

4. ROLES AND RESPONSIBILITIES SUMMARY

4.1 AP&SD AP&SD is responsible for the development of policies & procedures for SoD relating to processes that have significant financial impact. In addition AP&SD is the custodian of the SoD Rule Books that implement these policies and procedures in the SoD system, and will review and approve changes proposed to the Rule Books by other proponent or end user organizations.

4.2 EDPD. Computer Applications / EDPD is responsible for the development of policies and procedures relating to the administration, security and availability of the SoD system, the supporting landscapes and data. In addition EDPD will monitor the performance of the SoD system and support the automated and manual SoD prevention procedures.

4.3 CAD, SSAD, HAD. The application departments will comply with relevant policies and procedures relating to SoD, and provide the necessary support to proponents and end user organizations when analyzing existing and new business processes for potential SoD violations or risks.

4.4 Internal Auditing. Review and test SoD Rules, Compensating Controls for accuracy and completeness and monitor the effectiveness of SoD remediation activities during audit reviews.

4.5 Proponent Organizations. Develop and implement SoD rules for finance related processes under their control by working with AP&SD and SAP application departments to identify the relevant processes and building the required Rule Books and Rules to maintain an effective SoD implementation in these processes.

4.6 End User Organizations. Remediate the SoD violations in their organizations and participate in the development of the rule books for their processes.

4.7 COD. The Computer Operations Department is responsible for the hosting of the SoD database system and providing standard services for the system, for example backup, recovery, and other system administration activities.

5. MAINTENANCE AND ADMINISTRATION OF SoD DATABASE SYSTEM

5.1 SoD Server Administration: Computer Operations Department will maintain the SoD server, the application software and any SoD system interfaces. Examples of interfaces are SoD authorization data extracts of SAP authorization data and the automated interface between the SoD system and UAMT.

5.2 SoD System Upgrades: AP&SD is responsible for the coordination of upgrades and enhancements of the SoD system software and servers with EDPD and Computer Operations Department (COD). COD is responsible for implementing the upgrades and

enhancements, and AP&SD is responsible for the approval and acceptance of the upgrades and enhancements.

5.3 SoD System Access: Proponent and user access to the SoD system rule books and reports will be maintained by AP&SD. However, EDPD and Computer Operations Department will need to have Super User access to schedule and verify extracts and analysis; to troubleshoot issues and to perform any general maintenance activities.

5.4 Control of Super User Access: Because the SoD system does not allow for an administration access that is separate from rule book maintenance, there are some concerns that allowing permanent access at this level may introduce a risk where rule books or rules might be unintentionally changed or deleted. To mitigate against this risk, Super User access to the SoD system can only be granted through a Remedy System request, and the Super User ID must be checked out and in from SAP in the same way regular SAP Super IDs are checked out and in. A full audit trail of all changes made within the SoD system must be generated at the check in of the Super ID and attached to the Remedy Case as part of the resolution documentation. Until such time as we have a SoD system with more fine grained access control it will be necessary to follow this procedure.

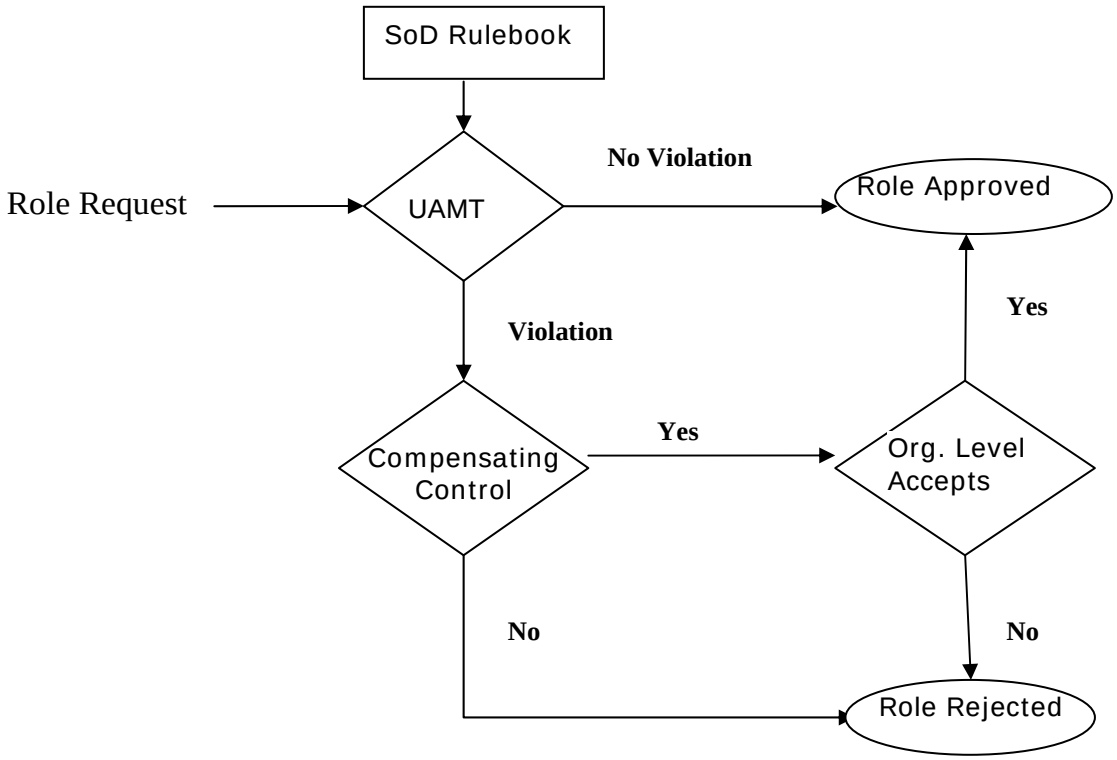
During the SoD system go live and system upgrades there may be an agreed period during which Super User access to the SoD system is granted to support staff on an ongoing basis for efficiency reasons. This period will be determined by AP&SD in agreement with EDPD and Computer Operations Department.

Approved: Original Approved by R.A. KRYGSMAN
R.A. KRYGSMAN, Manager
Accounting Policies &
Systems Department

PWA

DAZ/AAR

Appendix: Segregation of Duties (SoD) Prevention Process for User Assignments.



The SoD UAMT prevention process for user role assignments is designed to identify potential SoD authorization conflicts at the time a new SAP role is requested.

SAP roles are requested through the Corporate Portal and processed through the User Access Management Tool (UAMT). The UAMT filters the request through the rules in the SoD rulebooks. Four possible outcomes will result. In the most likely scenario, no violation will be detected. In that case, the request will be processed and the authorization will be granted provided the requester's management approves the request.

If a SoD violation is detected, the request will be rejected if there is no compensating control associated with the violation. This rejection is automatic. The request is not forwarded to management. The requester is notified of the reason for the rejection.

The last two scenarios, the violation has a compensating control. This means that there are circumstances that permit a requester to have authorizations which normally should be held by different individuals. The requester's management is asked to review the violation and the compensating control. If the management approves the request, then they are also verifying that the compensating control is in place and therefore misuse of the conflicting authorizations is unlikely. If the requester's management is not willing to verify the existence of the compensating control, then the request is rejected and the requester is notified of the reason for rejection.