Segregation of Duties Review (SOD Review)

Description and Workflow Configuration

Segregation of Duties Review (SOD Review)

Segregation of Duties Review is a process where the system checks periodically for any risk and violations associated with a user or functions. This functionality can be used during the initial clean-up of risk violations as well as a long-term strategy to review and affirm previous Mitigation assignments.

When SOD review is performed, it generates requests automatically, based on organization’s internal policy. SOD review provides Workflow Based review and approval process.

Purpose

This document will explain complete functionality of SOD review.

SOD Review Overview

Key feature of SOD Review:

- Decentralized review of Segregation of Duties violation.
- Workflow request for Access Review and approval
- Reaffirmation of Mitigation Control assignment
- Audit trail and Report for Audits

SOD Review Process

- There is a background job which generates SOD Review request.
- The system sends SOD review notification to reviewers.
- The reviewer review the request and perform the following option.
  - Reject Request Items
  - Mitigate Risk by assigning Mitigation Control.
  - Remove Access for items that are creating violations.
- There is one more optional step where we can involve Admin for Admin review before sending request to reviewers

SOD Review Process Explanation

- Admin Review.
  - There is an option for Admin Review which provides administrator to validate request data after request are generated (by SOD review job) but before generating Workflow task (but prior SOD Review update Workflow job). If any reviewer information is mission or need to be modify then Admin can do so before generating workflow, or can also delete requests if required
- Review Stage
  - We can specify whether Reviewer stage is addressed by user’s Manager or Role Owner.
- Security Stage: We can also include Security stage if required.

Workflow Stage Configurations

After deciding which stage to include in the SOD review workflow, we need to determine the specific behavior for each stage to reflect the review process. Like

- Email Notification
  - First of all we need to determine the content of the email notification to be send to approver of each stage. Recipient also needs to be determined.
- Reminder
  - We can also set Email reminder in this case. We can specify the interval of reminder notification.
- Escalation
  - You can specify Escalation on each stage based on time spent in a particular stage. If a Reviewer does not complete his review within the time specified in the date parameter defined in configuration, then the request will be escalated. The Audit log will
show this escalation. We can also specify whether escalation automatically removes the access that is not approved by a certain date.

Roles in SOD Review

The following role can appear in SOD Review Request

- **Administrator**
  - Administrators perform SoD Review-specific administrative tasks such as performing an Admin Review before generating a workflow for the request
- **Reviewer**
  - Reviewers are approvers at the Reviewer stage. A Reviewer can be a User’s Manager or the Risk Owner
- **User’s Manager**
  - User’s Manager is the direct manager of a particular user, as defined in the User Details Data Source.
- **Risk Owner**
  - Risk Owner is the owner specified in your Risk Analysis and Remediation (RAR) master data.
- **Coordinator**
  - Coordinators are users assigned to one or more Reviewers. Coordinators monitor the SoD Review process and coordinate activities to ensure that the process is completed in a timely manner

Prerequisites

The following jobs should be executed in the below sequence before running SOD review Jobs.

- Repository sync for User, Role, Profile (SPRO->GRC->Access Control->Synchronization Jobs-> Repository Sync)
- Action Usage Report (SPRO->GRC->Access Control->Synchronization Jobs-> Action Usage Sync)
- Role Usage Sync (SPRO->GRC->Access Control->Synchronization Jobs-> Role Usage Sync)
- Also make sure that Risk Owners are maintained.

Configuration Settings

This section will explains you SOD Review Configuration settings

IMG Configuration

Before running SOD review job there are some IMS settings that needs to be done

Go to IMG->GRC->Access Control-> Maintain Configuration Settings->

1. For PARAM “Risk Analysis” : Set Parameter 1027 Enable Offline Risk Analysis to YES
2. For PARAM “SOD Review” : Set the below Parameters
   1. 2016 **Request Type for SOD** : Choose Default Request type for SOD
   2. 2017 **Default Priority for SOD** : Choose Default Priority for SOD
   3. 2018 **Who Are Reviewers** : Choose Role Owner/Managers
   4. 2019 **Admin Review required before sending task to Reviewer** : Choose YES/No
   5. 2020 **Number of unique line items per SOD request** : Maximum value of this parameter can be 9999. Beyond 9999, the request will get split and all items will be moved to a new request. This parameter is introduced in GRC10.0 SP17 (SAP Note # 1994429)
   6. 2021 **Is actual removal of role allowed** : Choose Yes/No
Managing Coordinators

Go To NWBC-> Access Management-> Compliance Certification Review->Manage Coordinators

Screen will open. Now select any line item to change or create a new one.

Specifying Escalations

Go To SPRO->GRC->Access Control->User Provisioning->Maintain Service Level Agreement
Here you can create SLA for SOD review process. You can specify this via type Fixed by Date or Fixed by number of days and Formula.

Generating data for Request

For generating data for SOD review you need to schedule a job from NWBC-> Access Management ->Scheduling-> Background Scheduler
You can give Job Name and select “Generate data for Access Request SOD Review” and click on next.

After clicking on Next screen you can give the parameters for which you want to run this job.
Now, on clicking Next and then Finish the job will be scheduled.
You can check this job under NWBC -> Access Management -> Scheduling -> Background Jobs

Request Review

This step is only required if you have enabled Admin Review option.

The administrator reviews the requests to ensure completeness and accuracy of the request information prior to sending to Reviewers.

Go to Access Management -> Compliance Certification Review -> Request Review
On the Request Review screen, search for the SoD Review requests by selecting the SoD Risk Review Workflow and then review the data to confirm the Reviewer and Coordinator information is accurate.

On this screen you can enter information about the reviewer to the requests if not available.

An Administrator can also cancel the request if SoD Reviews are not required or if there is incorrect data.

**Update Workflow Job**

This step is only required if you have enabled Admin Review and the Admin Review has been completed.

Execute the SoD Review Update Workflow Job to push the workflow tasks to the Reviewers.

- Go to Access Management ->Scheduling->Background Scheduler.
- Click Background scheduler.
- The Schedule-Access Management Screen will appear.
- Choose Create to create a new request for Update Workflow.
- The Create Schedule screen will appear.
- Enter Schedule Name.
- Select Schedule Activity from the dropdown list. For SoD Requests, select Update Workflow for SoD Request.
Choose Finish.
- Go to Request Review, and check the status of the request if it has been completed.
- After completing all of the above mentioned steps, the requests will now come to the Reviewer’s Work Inbox to work on it.

Now you can view that request in the Work inbox. On opening the request it will look as below.

Since YES was selected for Actual removal of Roles during the configuration process, the “ACTUAL REMOVAL” pushbutton appears on the screen. If NO was selected, then the “PROPOSE REMOVAL” push button appears instead.
By selecting Risk and then choosing the “Actual Removal” pushbutton, you can remove the actual role associated with this Risk. By choosing the “Propose Removal” pushbutton you can only propose the removal, no actual removal is done on any roles. Choose Submit to complete the Review process.

**Workflow Configuration**

To process SOD review, you need to set the workflow settings from MSMP.

**Process ID:** SAP_GRAC_SOD_RISK_REVIEW

You can maintain Rule at the 2nd step. You can configure Function Module rules, BRF plus rules, ABAP class-based rules, and BRF plus flat rules.

The rules can be one of the following types:

- **Initiator Rule:** To check which path your request will take
- **Routing Rule:** To direct your request to take a detour
- **Agent Rule:** To check for agents (Reviewers) for the request in a particular stage
- **Notification Rule:** Used for notification purposes only

At the 3rd step you can define Agent

The possible agent types are:

- Directly Mapped Users: A group of users created within the workflow configuration
- PFCG Roles: All users who have specified PFCG role assignments
- PFCG User Group: All users who are part of the specified PFCG group
- GRC API Rules: All users returned by the configured rule for agents
Once the agents are maintained, choose the NEXT pushbutton to maintain the VARIABLES AND TEMPLATES.

In this screen, you can maintain custom notification templates as well as their variables and reminders.

Next step is to maintain paths.
Select a path and choose the ADD or MODIFY pushbuttons to define the path stages.

In the Maintain Stages table, choose the MODIFY TASK SETTINGS button to change the stage settings.

In the Approval Type column, select All Approvers or Any One Approver from the dropdown list. This determines if all approvers or any one approver is required to approve the stage.

If you choose Yes for Escalation, specify the escalation setting by entering the idle time in minutes. Idle time is the amount of time by which, if the stage is not approved or rejected, the task is either sent to the specified agent or the workflow moves to the next stage.
Choose the NEXT pushbutton to go to the Maintain Route Mapping screen. In this step you can maintain route mappings between the initiator rules result and the actual path for the result.

Now Generate MSMP version

**Checking SOD Review Requests**

After a request is generated, it is sent to the reviewer’s Work Inbox and can be accessed by performing the following steps:
You can also search this request under Search Request-> Select Process ID as SOD Risk Review Workflow

Managing Rejection

The line items that are rejected by an approver can be accessed and reworked from the Managing Rejections screen.

Go To Access Management ->Compliance Certification Reviews-> Manage Rejections.
Select the Process Type and click on Search

You can find the rejections on this screen.

**Related Documents**

There are many major SOD review fixes after SP14 GRC 10.0

Below are the important SAP Note regarding this.

1994429 - UAM: Running Batch Risk Analysis is mandatory for SOD Review Request creation

2057848 - UAM: Incorrect value is displayed for the Variable REQUESTER_NAME in the SOD Notifications

2058766 - Removal of reviewer not possible from request reviewer

1888260 - UAM: Issues with SOD Review request

1973155 - Providing table sorting option in SOD Review request and mitigations not saved on saving SOD request