Access Control 5.3
Segregation of Duties Review

Applies to:

Access Control 5.3

Summary

GRC Access Control identifies and prevents access and authorization risks in cross-enterprise IT systems to prevent fraud and reduce the cost of continuous compliance and control. This document discusses the Segregation of Duties Review feature introduced in AC 5.3 including it benefits, configuration, use of the feature and workflow options.

Author: Ankur Baishya, Regional Implementation Group
Lori Donnelly, Customer Advisory Office

Company: Governance, Risk, and Compliance
SAP BusinessObjects Division

Created on: 1 December 2009

Version 1.1

Typographic Conventions

Type Style	Description
Example Text	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation
Example text	Emphasized words or phrases in body text, graphic titles, and table titles
`Example text`	File and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example text`	User entry texts. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example text>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE TEXT`	Keys on the keyboard, for example, F2 or ENTER.

Icons

Icon	Description
	Caution
	Note or Important
	Example
	Recommendation or Tip

Table of Contents

1. Management Overview

The Segregation of Duties Violation Review (SOD Review) feature of Access Control (AC) automates and documents the periodic decentralized review of SOD violations by business managers or risk owners. It can be used during the initial "Clean-up" of SOD violations as well as a long-term strategy to review and affirm previous mitigation assignments. Requests are generated automatically based on the company's internal control policy. It provides a workflow-based review and approval process. This document provides details on functionality of the feature, its process options, configuration, and use.

The following abbreviations are used throughout this document to represent the capabilities of AC:

- CUP Compliant User Provisioning
- ERM Enterprise Role Management
- RAR Risk Analysis and Remediation
- SPM Superuser Privilege Management

2. Key Features and Benefits

The key features of the Segregation of Duties Review (SOD Review) in AC 5.3 are:

- Decentralized review of segregation of duties violations.
- Reaffirmation of mitigating control assignments.
- Workflow of requests for review and approval.
- Status and history reports to assist in monitoring the review process.
- Audit trail and reports for supporting internal and external audits.
- Support for back-end systems connected to Access Control as well as legacy systems.

The key benefits of the SOD Review are:

- A streamlined internal control process with collaboration among business managers, internal control, and information technology teams.
- Improved efficiency and visibility of the internal control process.

3. Technical Prerequisites

The Segregation of Duties Review feature was introduced in Access Control 5.3. Therefore, you must have version 5.3 installed to utilize SOD Review with SP06 or higher recommended. The screenshots provided in this document are from an AC 5.3 SP09 system. Use of the SOD Review feature requires configuration in multiple capabilities.

- Configuration of connectors in RAR is required for alert generation to provide usage information. In addition, a full batch risk analysis must be executed to produce the violation data used to generate SOD Review requests.
- Configuration of connectors, the SOD Review feature, and workflow for the requests is required in CUP.

The configuration section of this document provides more details.

Another prerequisite is having a user detail data source to provide the manager relationship for the users included in the review. This data source may be an SAP ERP HR system or an LDAP (Lightweight Directory Access Protocol). Details are discussed in the AC 5.3 Configuration Guide.

4. Review Process

This section discusses the review process and the decisions to be made regarding how you will use the review process. A later section will discuss how to configure the system to reflect the chosen process. SOD Review is currently supported for any system that has risk analysis results available in RAR.

4.1 Overall Process

4.1.1 SOD Management by Exception

For new implementations, the SOD Violation Review reports unmitigated SOD violations in the target system and uses workflow to route requests for review as to whether to remove the violation by modifying access or to mitigate the risk when violations are necessary. In the case of remediation, the reviewer specifies the access to be removed. The request is ultimately sent to the security team for execution since this requires analysis of the assigned access.

This process is also followed for established implementations that are not using the full suite of Access Control capabilities or that do not enforce compliant provisioning. The Administrator executes the job SOD Review Load Data without Mitigated Risks to create requests for this process.

4.1.2 Mitigation Reaffirm

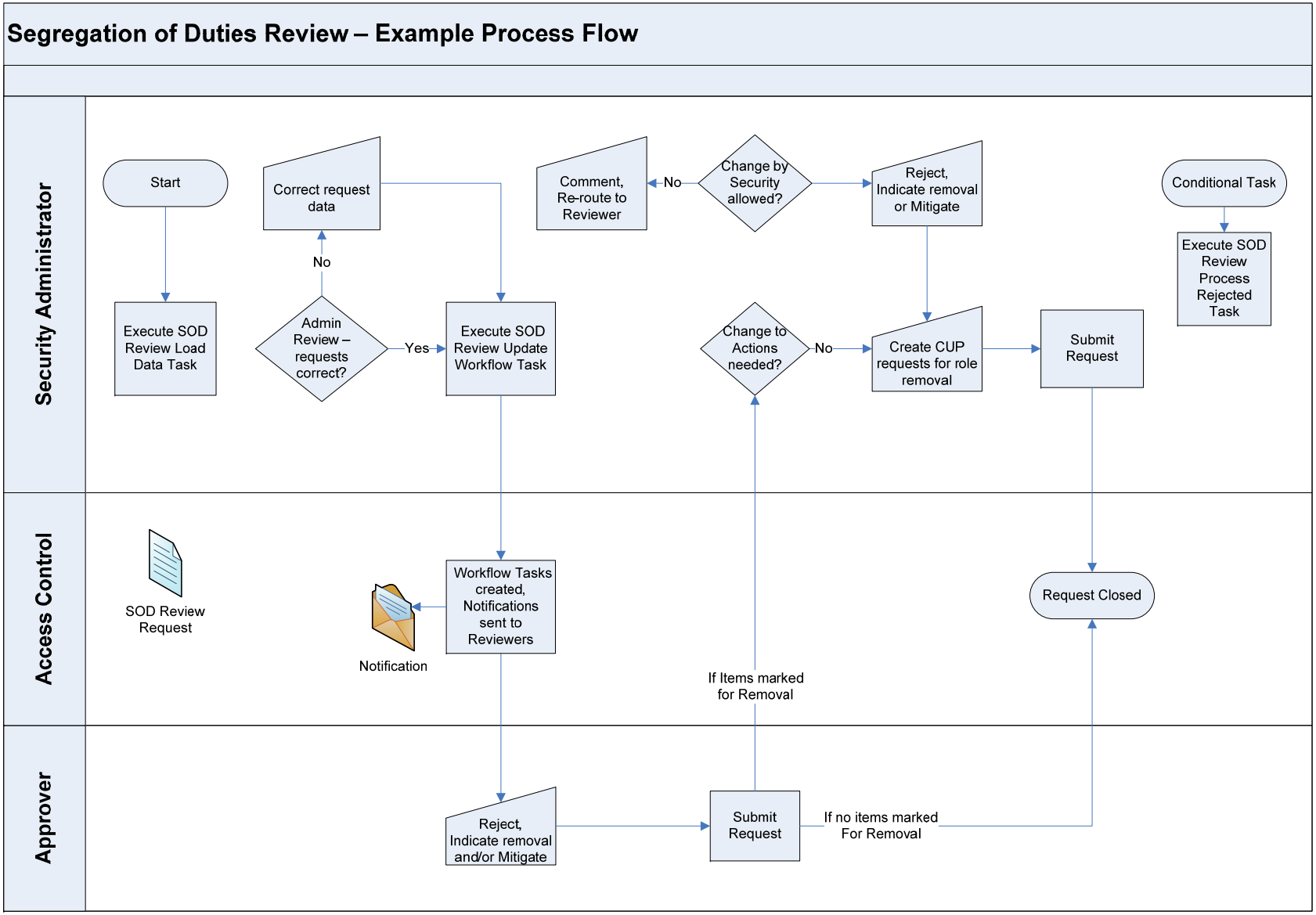
For established implementations that are following the preferred practice of compliant provisioning in a clean environment, the SOD Violation Review reports mitigated SOD violations in the target system and uses workflow to route requests for periodic review and determinate whether the violation is still necessary for the user and that the mitigation assignment is still relevant. If appropriate, the mitigating control assignment is extended are reaffirmed. This use follows the same process as the SOD Risk Review but the requests will include the user's mitigation control assignments. The Administrator executes the job SOD Review Load Data with Mitigated Risks to create requests for this process.

4.1.3 SOD Review Process Flow

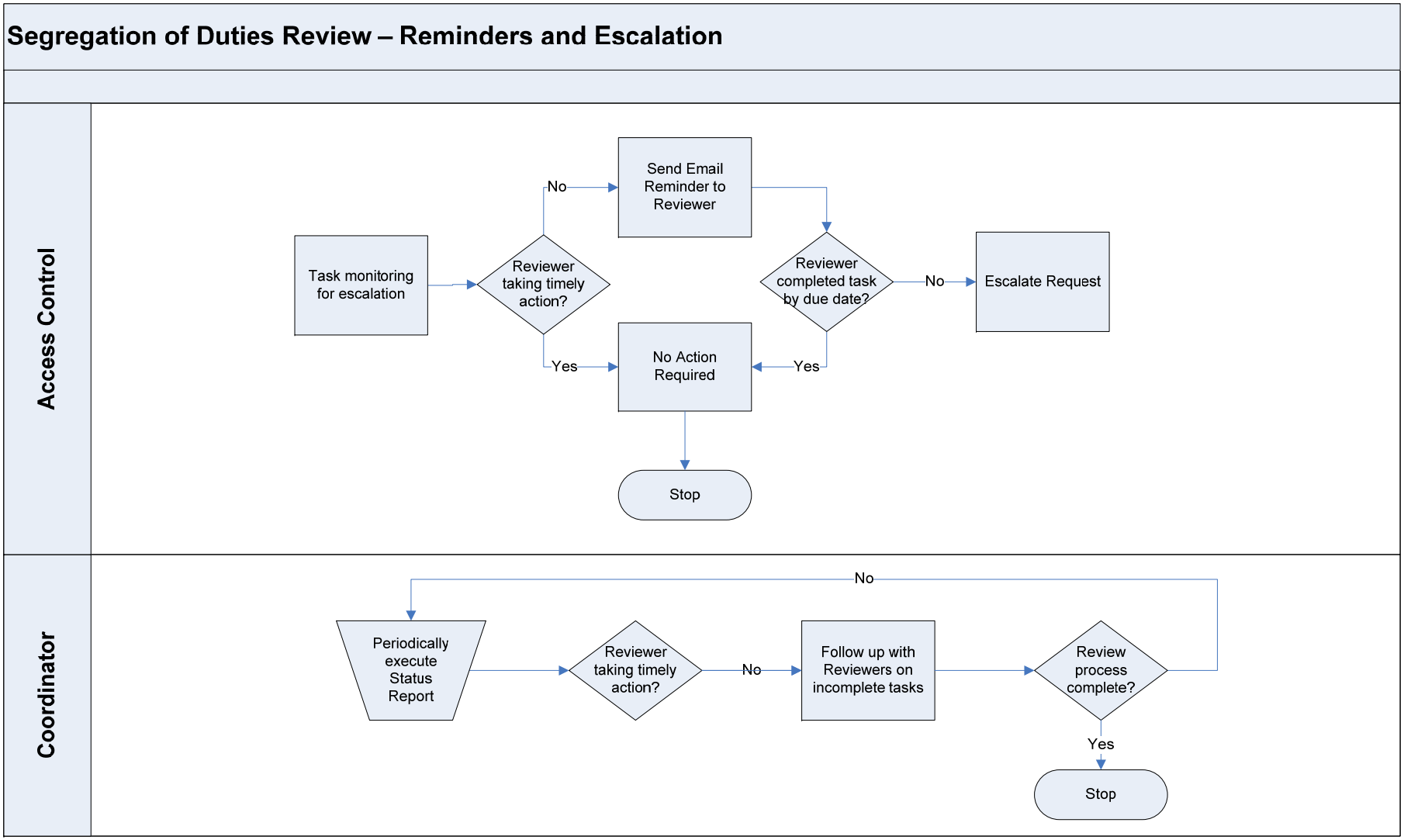
The high-level process for SOD Review is as follows.

- Batch risk analysis is executed.
- SOD Review requests are generated.
- E-mail notifications are sent to reviewers.
- Requests are reviewed and actions are noted by the reviewer to propose the removal of a function, assign a mitigating control for the risk, or confirm the existing mitigating control assignment.
- Mitigating control assignments or extensions are automatically executed.
- Functions marked for removal are analyzed and addressed by Security.

The detailed process for executing the SOD Review is depicted below. The first diagram shows the flow for a common SOD Review. The second diagram shows the activity being performed by Access Control to send reminder notifications or escalation requests as dictated by configuration when the stage approver does not submit completed requests and requests are not closed within the time defined in configuration.



4.1.4 Escalation Process Flow



4.1.5 Roles in the SOD Review Process

Administrator: This person has the AE_Admin UME role assigned for Access Control. They can perform general CUP administrator tasks in addition to SOD Review-specific administrator tasks, such as cancelling SOD Review requests and regenerating requests for rejected users.

Reviewer: This term refers to the approver at a particular stage. The *Reviewer* may be the user's manager, a role owner, a security team member, or an Access Control administrator.

User's Manager: The direct manager of a user as defined in the *User Details Data Source.*

Risk Owner: The risk owner specified in RAR master data.

Coordinator: The *Coordinator* specified in CUP master data. The *Coordinator* is assigned to *Reviewer*. They monitor the SOD Review process and coordinate activities to ensure the process is completed in a timely manner.

4.2 Process Options

Multiple process options will determine the approvers of the SOD Review requests.

4.2.1 Admin Review

You decide whether to enable *Admin Review.* This configuration option provides an opportunity for the administrator to validate the request data prior to executing the *SOD Review Update Workflow* job. If the manager or role owner information is incorrect or missing, the administrator can modify the data prior to generating workflow tasks and notifications. The administrator can also cancel requests.

4.2.2 Reviewer Stage

You decide whether the Reviewer stage will be addressed by the User's Manager or the Risk Owner.

4.2.3 Security Stage

You decide whether to have a security stage. A security stage is suggested as removal of functions from Users will have to be executed, if applicable.

If a security stage will be included in your approval workflow, you must decide whether security personnel will be able to modify the direction previously noted by an Approver.

4.2.4 Additional Approver Stage

You decide whether you will have an additional stage with the approver derived by a Custom Approver Determinator (CAD). The fields available in the SOD Review CAD differ from those available in the standard CUP CADs. The fields available are in the SOD Review CAD are:

- Application
- Request type
- Priority
- Risk(s) being reviewed

For more details on the use of CADs, see the Configuration Guide.

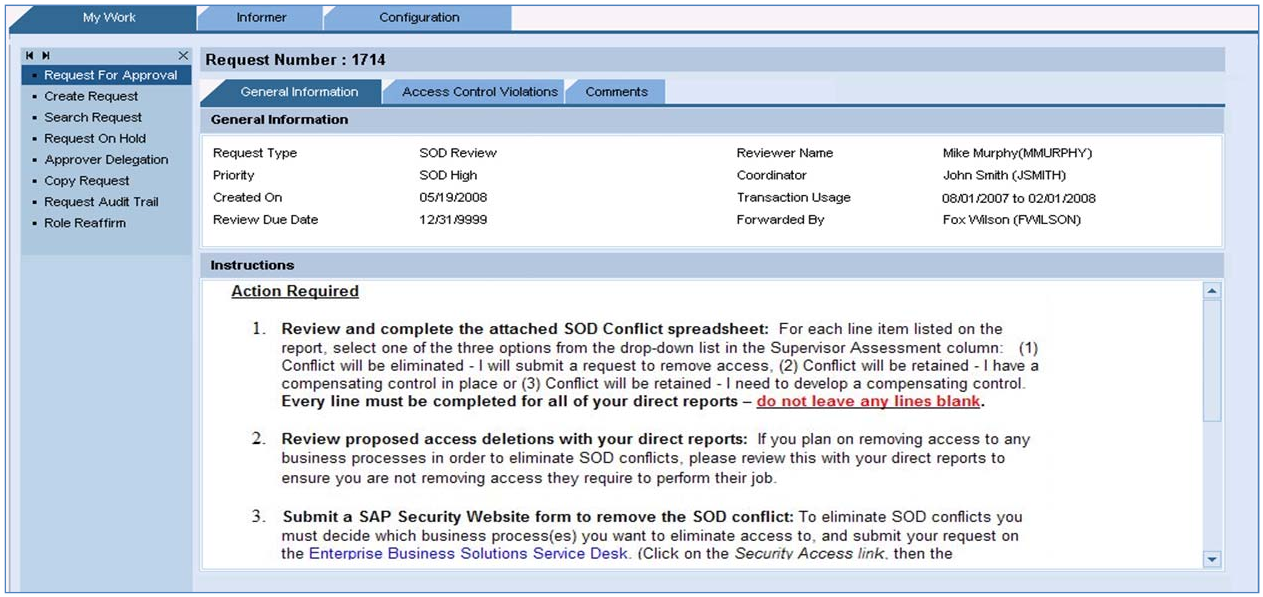
4.2.5 Treatment of Mitigated Risks

You decide whether mitigated risks will be included in the SOD Review. Including mitigated risks may be used for periodic review and reaffirmation of existing mitigating control assignments. This decision impacts configuration of risk analysis in RAR.

4.2.6 Instruction for Reviewers

You can provide detailed instructions for reviewers to supplement the content of the notification emails. The level of instruction for approval of periodic access reviews might be more extensive since it is an infrequent process and may involve reviewers who do not perform routine approval of requests to create or change accounts.

The *Instructions* area of the SOD Review requests is an HTML viewer. An example of an SOD Review request with an HTML page provided in the request is shown here.



4.3 Workflow Stage Configuration

Now that you have decided which stages to include your SOD Review workflow, you must decide on specific behavior for each stage to reflect your review process. The items to be addressed in configuration are listed below.

4.3.1 Email Notification

You decide on the content of email notifications to be sent to the approvers at each stage. You determine the recipient(s), the content of the notification header and the email body. For more details, see the email notification configuration section below or see the Access Control 5.3 Configuration Guide.

4.3.2 Reminders

You decide whether to send reminders to the reviewers who have not completed their portion of the request by the date specified in configuration. You can specify the interval of reminder notifications in days, the reminder notification header, and body content. For details on configuring reminders, see the configuration Guide.

4.3.3 Escalation

You decide whether to escalate SOD Review requests in each stage's details. Therefore, escalation is based on the time spent in a particular stage. If a reviewer does not complete their review of a request according to the date parameter defined in configuration, then the request is escalated. Escalation of a request will show in the request's audit trail.

You also determine whether escalation will include automatically removing access that is not approved by a certain date.

5. Configuration and Master Data

This section contains instructions for configuring the SOD Review and providing the necessary master data. It includes many excerpts from the *AC 5.3 Configuration Guide.* For more information on general configuration, please review the corresponding section of the configuration guide.

5.1 Configuration and Master Data in RAR

5.1.1 Define Connector(s)

You must define connectors for systems to be included in the SOD Review process. This is required to perform batch risk analysis for systems that are supported with Real-Time Agents (RTAs) and for systems that are not supported with RTAS. It is also required to support alert generation. Navigate to *Configuration → Connectors* to define the required connectors. For more information on defining connectors, please refer to the configuration guide.

5.1.2 Define Risks

Segregation-of-duties rules must be generated to be used in performing batch risk analysis for systems to be included in the SOD Review process. Maintain the risk and function definitions for the rule set to be used for batch risk analysis and generate the rules. Please note that critical access risks are not included in the SOD review process. You may view critical access risk violations in management reports and in ad-hoc risk analysis.

5.1.3 Configure Default Rule Set

You must specify the default rule set in RAR. This rule set will be used by batch risk analysis and, therefore, will be the foundation of violations reported in the SOD Review requests. Navigate to *Configuration → Risk Analysis → Default Values → Default rule set for Risk Analysis* to specify the rule set to be used for batch risk analysis. You should consider the requirements of CUP and ERM in addition to the SOD Review requirements since all functions use the default rule set specified in RAR.

5.1.4 Configure Exclusion of Mitigated Risks

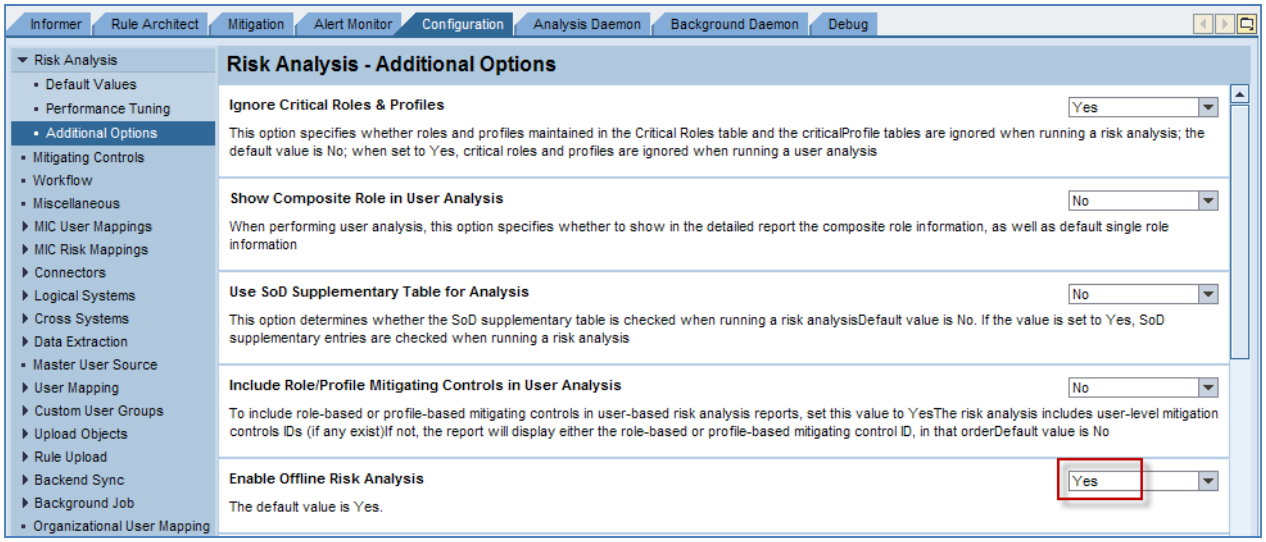
You must configure whether mitigated risks will be excluded from the batch risk analysis and, subsequently, the offline analysis tables. If the data is excluded in RAR, it will not be available to be included in the SOD Review Requests. Navigate to *Configuration → Risk Analysis → Default Values* to maintain this parameter.

5.1.5 Configure Users to be Included in Batch Risk Analysis

You must indicate the users to be excluded from the batch risk analysis and, subsequently, the offline analysis tables. If the data is excluded in RAR, it will not be available to be included in the SOD Review Requests. You can choose to exclude locked users and expired users. Navigate to *Configuration → Risk Analysis → Default Values* to maintain these parameters.

5.1.6 Enable Offline Analysis

Offline Analysis must be enabled as it is the source of risk violation information for SOD Review requests. Enabling offline analysis causes the batch risk analysis results to be stored in the offline analysis data tables. Web Service calls from CUP extract the offline analysis results during the SOD Review Load Data with/without Mitigated Risks job and populate the SOD Review requests with this data. Navigate to *Configuration → Additional Options* to enable Offline Analysis.



5.1.7 Configure Exclusion of Critical Roles/Profiles

If you have roles or profiles that introduce a large number of risk violations, such as SAP_ALL and roles that provide OSS or Basis team members extensive access, those roles and profiles should be excluded from Batch Risk Analysis and should be monitored by reviewing assignments of those specific roles/profiles. Including these roles/profiles in batch risk analysis will result in large volumes of data being stored in the offline analysis results tables and may negatively impact system performance.

Navigate to *Configuration → Risk Analysis → Additional Options → Ignore Critical Roles & Profiles* to maintain this parameter.

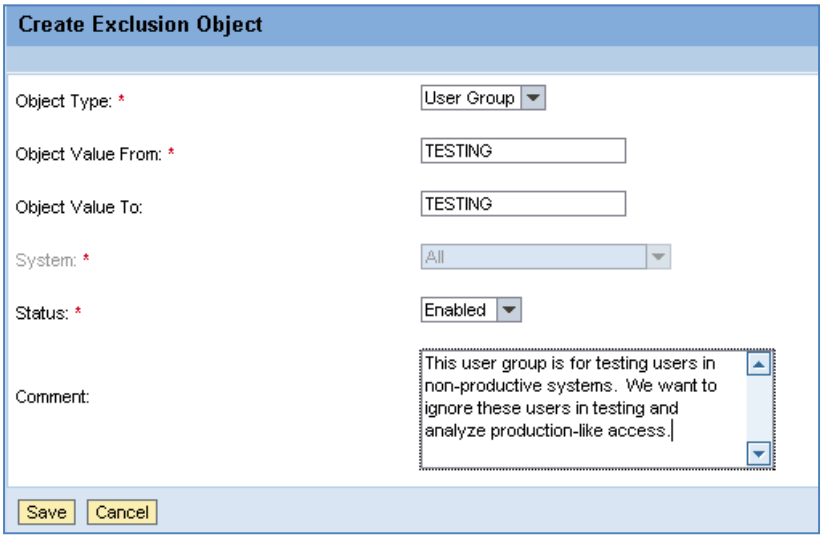
5.1.8 Identify Critical Roles/Profiles

If you have configured Access Control to exclude Critical Roles/Profiles, then you identify the roles and profiles to be excluded. Navigate to *Rule Architect → Critical Roles* or *Critical Profiles* to maintain the list objects. Entries populated here will not be useful without the associated parameter being selected.

5.1.9 Identify Exclude Objects

In addition to excluding critical roles or profiles, you can exclude other items from batch risk analysis. This may be used to ignore users with excessive access, such as support team member accounts in a testing environment.

Navigate to *Configuration → Background Job → Schedule Job.* Choose *Exclude Objects.* Populate the information for the items to be excluded, and then choose *Save.* You may exclude Users, User Groups, Profiles and Roles. Please note that identifying an item as an exclude object for batch risk analysis will cause data previously populated for those items in the offline analysis or management report tables to be deleted with a subsequent update.



.

5.1.10 Alert Generation in RAR

Alert Generation data in Risk Analysis and Remediation provides the foundation of the usage information in the SOD Review requests for connected back-end systems. Other than the previously defined connector, there is no required RAR configuration to allow the system to obtain usage information automatically for systems supported by RTAs. The only requirement is that the connector ID in RAR must be identical to the connector ID in CUP. The SOD Review process does not currently provide usage information for systems that are not supported by RTAs.

5.2 Configuration and Master Data in CUP

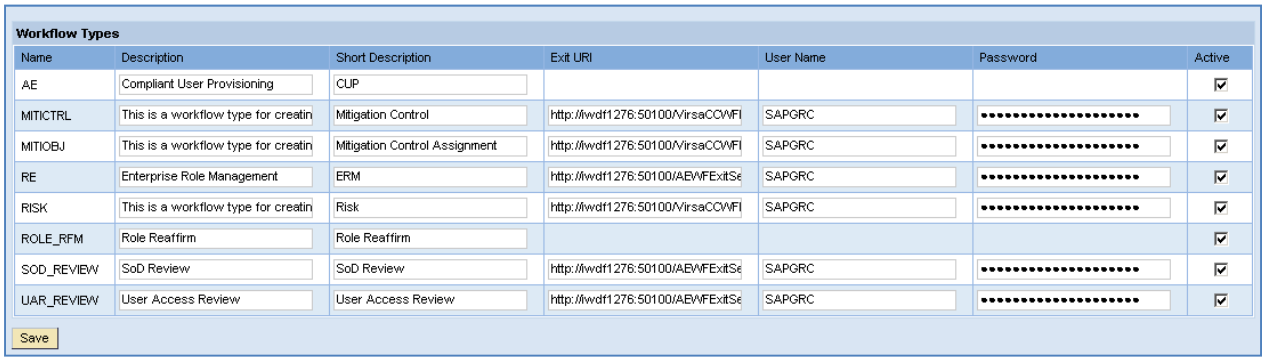
5.2.1 Upload Initial Data File for SOD Review

Ensure that the *AE_init_append_data_ForSODUARReview.xml* file has been uploaded in *Configuration → Initial System Data.* This .xml file is one of the initial data files included with Access Control.

Support Packages may deliver subsequent versions of the initial data files and you must be sure that you have the data files that correspond to your AC support package level. Upload the specified initial data file in CUP using the *Append* option. If you are configuring a new Access control installation, then you will need to upload all initial data files.

5.2.2 Maintain Workflow Type

You must create a Workflow Type for the Segregation of Duties Review. Navigate to *Configuration* → *Miscellaneous*. In the Workflow Types pane, maintain the entry *SOD_REVIEW*.



Workflow Types

Name	Description	Short Description	Exit URI	User Name	Password	Active
AE	Compliant User Provisioning	CUP				☑
MITICTRL	This is a workflow type for creatin	Mitigation Control	http://wdf1276:50100/VirsaCCWFI	SAPGRC	••••••••••••••••••••	☑
MITIOBJ	This is a workflow type for creatin	Mitigation Control Assignment	http://wdf1276:50100/VirsaCCWFI	SAPGRC	••••••••••••••••••••	☑
RE	Enterprise Role Management	ERM	http://wdf1276:50100/AEWFExitSe	SAPGRC	••••••••••••••••••••	☑
RISK	This is a workflow type for creatin	Risk	http://wdf1276:50100/VirsaCCWFI	SAPGRC	••••••••••••••••••••	☑
ROLE_RFM	Role Reaffirm	Role Reaffirm				☑
SOD_REVIEW	SoD Review	SoD Review	http://wdf1276:50100/AEWFExitSe	SAPGRC	••••••••••••••••••••	☑
UAR_REVIEW	User Access Review	User Access Review	http://wdf1276:50100/AEWFExitSe	SAPGRC	••••••••••••••••••••	☑

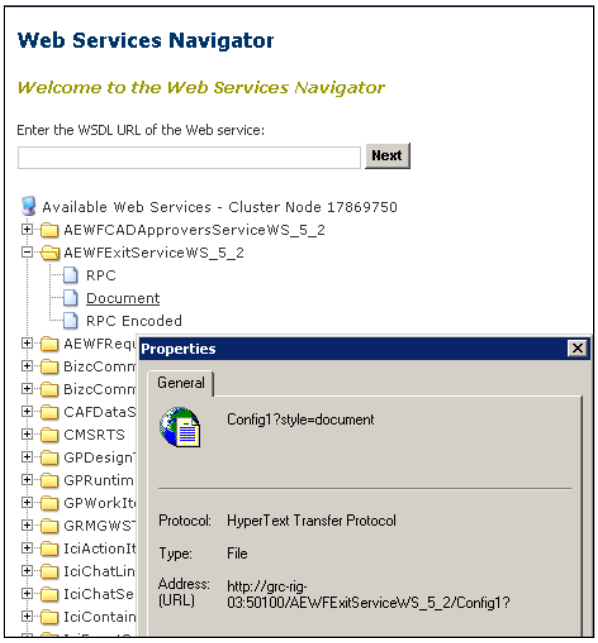
Save

Maintain the following fields:

- Description fields.
- *Exit URI* of the web service *AEWFExitServiceWS_5_2*.

  The format of the URI is http://***<server>:<port>***/AEWFExitServiceWS_5_2/Config1?wsdl.

  You may use the *Web Services Navigator* to identify the *Exit URI.* Expand the entry for AEWFExitServiceWS, right-click on *Document,* and select *Properties* to display the URI.



- *User Name* and *Password:* Enter the account and password to be used accessing RAR.
- *Active* indicator: Select the indicator to enable the connector.

5.2.3 Maintain Request Type

The initial data files include the *SOD_REVIEW* request type which must be activated.

- Go to *Configuration* → *Request Configuration* → *Request Type.*
- Select the *SOD_REVIEW* request type and select *Change.*
- Maintain the descriptions.
- Ensure that the *Active* indicator is selected.

5.2.4 Maintain Request Priority

Confirm that the *SOD_HIGH* priority is present and associated with the SOD Review *Workflow Type.*
Navigate to *Configuration → Request Configuration → Priority.*

Request Configuration

Priority

Priority	Short Description	Description	Workflow Type
HIGH	CUP - High	Compliant User Provisioning - High Priority	CUP
LOW	CUP - Low	Compliant User Provisioning - Low Priority	CUP
MC_HIGH	MITICTRL High	MITICTRL High	Mitigation Control
MEDIUM	CUP - Medium	Compliant User Provisioning - Medium Priority	CUP
MO_HIGH	MITIOBJ High	MITIOBJ High	Mitigation Control Assignment
RE_HIGH	RE High	RE High	ERM
RS_HIGH	High	High Priority for Create/Modify CC Risk	Risk
SOD_HIGH	SOD High	SOD High	SoD Review
UAR_HIGH	UAR	UAR High	User Access Review

5.2.5 Ensure Active Number Range

Ensure there is an active number range in CUP. The number range is applicable to all CUP requests and is not specific to any request type(s).

Go to *Configuration → Number Ranges* to maintain number ranges.

5.2.6 Configure Risk Analysis Integration with RAR

You must maintain configuration to allow integration of CUP and RAR to support risk analysis during the SOD Review process. Navigate to *Configuration → Risk Analysis*. Ensure the first two panes are configured (*Select Options* and *Select Risk Analysis and Remediation Version*).

Select Options

- *Default Analysis Type:* Permission level is recommended to avoid false positive SOD analysis results.
- *Consider Mitigation Controls* should be selected if you wish to distinguish between mitigated and unmitigated risks during the review process. It should also be selected if the mitigation assignment is to be reviewed or extended.

Select Risk Analysis and Remediation Version

- *Version:* Choose the entry that represents the version of your RAR capability
- *URI*: Provide the URI of the Risk Analysis WebService. You may use the *Web Services Navigator t*o identify the *Exit URI.* Expand the entry for VirsaCCRiskAnalysisService, right-click on *Document,* and select *Properties* to display the URI.
- *User Name* and *Password:* Logon information to access RAR
- *Perform Org. Rule Analysis:* Choose this entry is organizational rules have been created and should be considered in the risk analysis.

5.2.7 Configure Mitigation Integration with RAR

You must maintain configuration to allow integration of CUP and RAR to support mitigation during the SOD Review process if mitigating control assignments are allowed or desired. Navigate to *Configuration → Mitigation*.

Select Options

- *Allow Approvers to approve access, despite any conflicts:* Choose this setting if you allow introduction of new risks without mitigating control assignment
- *Default Duration for the Mitigation Control:* The number of days that will default for the mitigating control assignment. It may be changed at assignment.
- *URIs and URLs:* Maintain the following addresses. You may use the *Web Services Navigator t*o identify each address by expanding the entry shown below, right-clicking on *Document,* and selecting *Properties* to display the address.
    - *Mitigation URL: VirsaCCMitigation5_0Service.*
    - *Risk Search URL: VirsaCCRisk5_0Service.*
    - *Org. Rule Search URI: VirsaCCOrgRules5_3Service*
    - *Function Search URI: VirsaCCFunction5_0Service*
- *Mitigation of critical access risks required before approving the request:* Select this option if you require critical access risks to be mitigated.

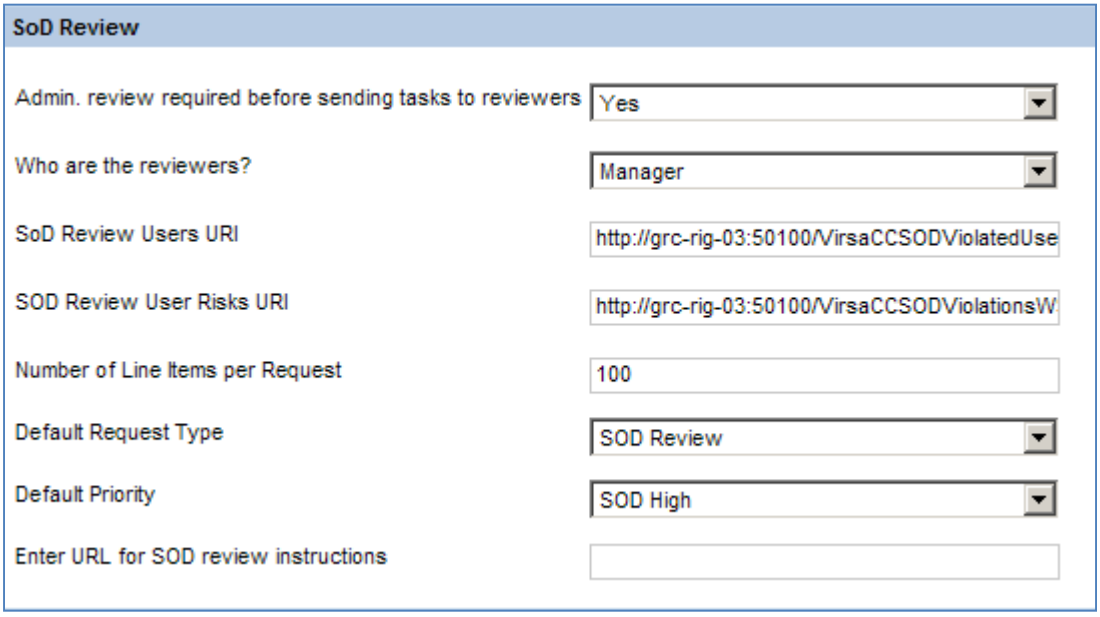
5.2.8 Maintain User Data Source

There are multiple types of data sources in CUP. You must identify a *Search Data Source* to be the source of all user IDs returned when performing a search. You may also identify a *User Details Data Source* that will be the source of all user-to-manager relationships. The *User Details Data Source* is required if your risk violations review process specifies the *User's Manager* as the *Reviewer*.

Go to *Configuration → User Data Source* to configure both types of data sources. For details on this configuration, see the *AC 5.3 Configuration Guide*.

5.2.9 Configure User Review

Go to *Configuration → User Review → Options* and specify the parameters for the SOD Review requests to be generated in the *User Review* pane.



1. *Admin. review required before sending tasks to reviewers:* Maintain this parameter based on the decision made when considering the process options.
   - *Yes:* The administrator reviews the SOD Review requests prior to the generation of workflow tasks. The administrator makes the required approver modifications and cancels any SOD Review requests that are not desired. This is recommended to ensure requests have proper reviewers and coordinators assigned before requests are distributed to reviewers.
   - *No:* The administrator does not have an opportunity to review SOD Review requests prior to sending the workflow notifications to reviewers.

   Note: If there are user records without a manager identified in the User Detail Data Source, then you must enable Admin Review to generate requests.
2. *Who are the reviewers?*
   - *Manager* represents the manager of the user as identified in the User Detail Data Source.
   - *Risk Owners* represents the risk owner identified in Risk Analysis and Remediation master data.
   -

   SOD Review Users URI: You must configure the web service location to identify users having risk violations.
   http://<server>:<port>/VirsaCCSODViolatedUsersWS/ConfigVirsaCCSODViolatedUsers?wsdl&style=document
3. SOD Review User Risks URI

   You must configure the web service location to identify the risk violations.
   http:://<server>:<port>/VirsaCCSODViolationsWS/configVirsaCCSODViolationsWS?wsdl&style=document
4. *Number of Line Items per Request* This is the maximum number of lines for user role assignments permitted on a request. If more lines are required than the maximum number allowed, then another request is required for the remaining items. Therefore, each reviewer may receive one, several or many requests depending on how many SOD violations they have to approve.

> **Note**
> If a user's violations cause the total lines of the request to exceed the maximum number of lines for a request, then that user's violations will cross requests.

5. *Default Request Type:* The dropdown list includes any request type in the system that has the *Segregation of Duties Review* workflow type.
6. *Default Priority* Set the default priority of the request to the value configured or confirmed earlier.
7. *Enter URL for SOD Review instructions:* If an HTML page with detailed instructions for reviewers was created to supplement any instruction in the email notification, enter the URL of that page. The page can be saved to a local directory of your choice on your internal server.
8. Click *Save*.

5.2.10 Maintain Rejection Reasons

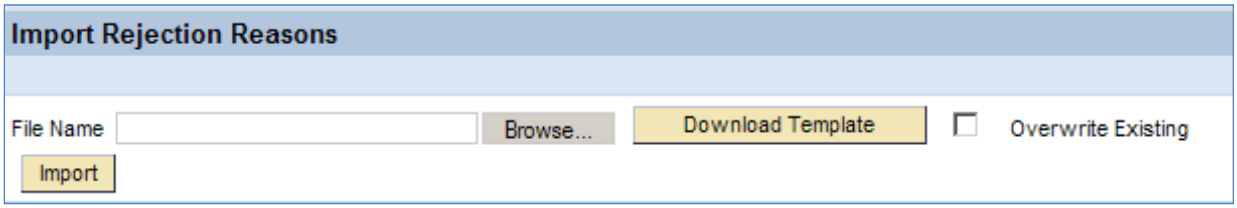
Rejection reasons are mandatory when rejecting a review request. You must upload the reason codes and descriptions using a template.

Procedure

1. Go to *Configuration → User Review → Reason for Rejection*. The new *Rejection Reason* screen appears.
2. Under *Import Rejection Reasons,* click *Download Template*. The template opens in Excel.
3. Complete the required information and save the template.

Field	Max Field Length	Recommendation	Possible Values
ReasonCode (required)	10 characters	All UPPER case No special characters, no spaces	Letters and numbers
ReasonEnable	n/a	Indicate whether the reason code is enabled	Yes/yes/y/YES/Y No/no/n/NO/N *(When empty default value No)*
ShortDescription_xx (XX – language code like EN, DE etc.)	100 characters, including spaces	Description maintained in the application's default language and other reviewer languages	Letters and numbers

4. Under *Import Rejection Reasons,* click *Browse.*



5. Select the rejection reasons file and click *Import.*

> **Note**
>
> You cannot delete reason codes from the application. To deactivate a reason code, set the *ReasonEnable* field as **No**, choose the *Overwrite Existing* option, and import the upload file.

5.2.11 Configure Workflow

You can configure an SOD Review workflow based on your organization's requirements. For example, the SOD Review workflow may consist of a primary path with a single stage for *Reviewer* approval and a

detour path. A common detour path has a single stage for *Security* approval with a detour condition for action of *Marked for Removal.*

This document illustrates a simple example of a Segregation of Duties Review workflow. The following steps are included in the example.

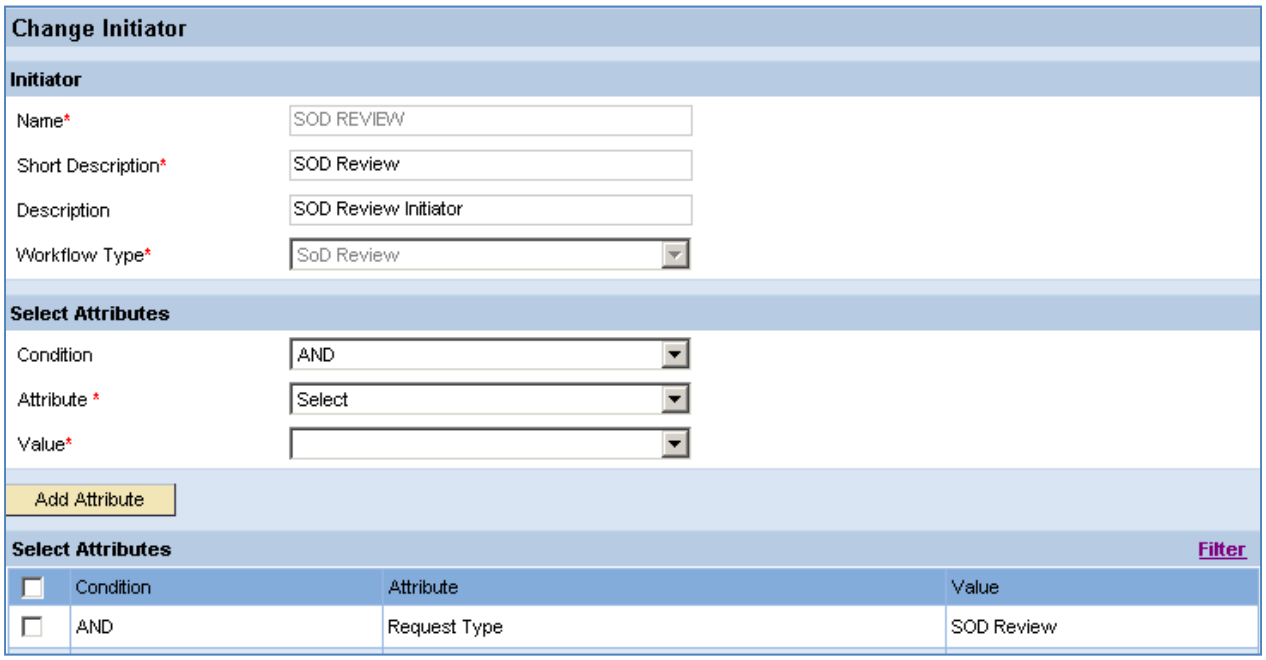
- Define an Initiator.
- Define Stages (one stage for *Reviewer* and another stage for *Security*).
- Define Paths (one path for a Reviewer and a detour path for Security).
- Define a Detour with condition.

5.2.11.1 Define an Initiator

The initiator specifies the conditions for sending access requests down a particular path. In this case, we will create an initiator for SOD Review requests.

1. Navigate to *Configuration → Workflow → Initiator.* The *Initiators* screen appears.
2. Click *Create*. The *Create Initiator* screen appears.
3. In the *Name* field, enter a name for your initiator. For example, enter '*SOD Review Initiator'*.
4. In the *Short Description* field, enter a brief description for this initiator.
5. In the *Description* field, enter a long description for this initiator.
6. In the *Workflow Type* dropdown menu, select *SOD Review*.
7. In the *Condition* dropdown menu, select the *AND* condition.
8. In the *Attribute* dropdown menu, select *Request Type*.
9. In the *Value* field, select *SOD Review*.
10. Click *Add Attribute*.
11. Click *Save*.

The result is the SOD Review Initiator definition.



5.2.11.2 Define Stages

For the example workflow, you will define one stage for the Reviewer (the user's manager or the risk owner in RAR) and one stage for Security.

1. Navigate to *Configuration → Workflow → Stage*. The *Workflow Stages* screen appears.
2. Click *Create*. The *Stage Configuration* screen appears.
3. In the *Name* field, enter a name for your stage. For example, enter <**SOD Reviewer**>.
4. In the *Short Description* field, enter a brief description for this stage.
5. In the *Description* field, enter a long description for this stage.
6. In the *Workflow Type* dropdown menu, select *SOD Review*.
7. In the *Approver Determinator* dropdown menu, select *Reviewer* (for User's Manager or Risk Owner).

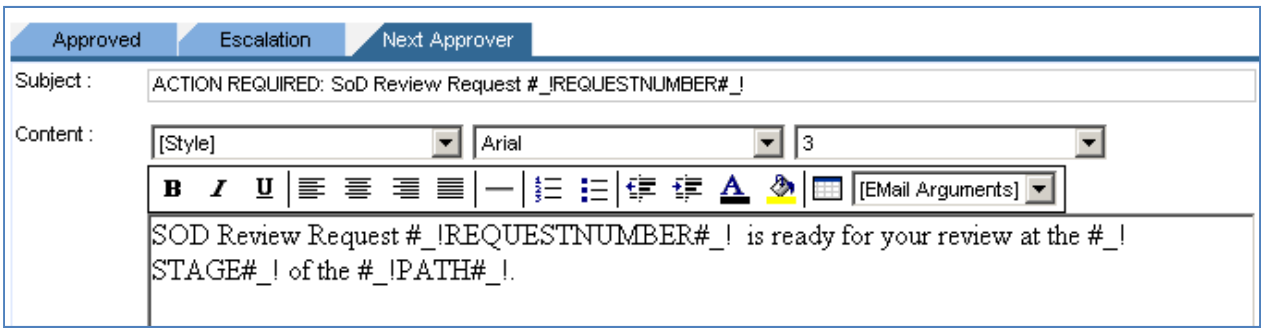
> **Note**
> Compliant User Provisioning provides two out-of-the-box approvers: *Reviewer* and *Security*. Optionally, you can define a Custom Approver Determinator (CAD) for a custom approver.

8. Specify the time desired for escalation in *Request Wait Time (Days)* and *Request Wait Time (Hours)*. This is the number of days and hours the request may stay in the stage before the request is escalated.
9. In the *Escalation Configuration* dropdown menu, select the type of action taken by the system when escalation is triggered. The following options are available:
   - *No Escalation:* Choose this setting when no escalation is required. *orward to Administrator:* Upon escalation, the request is sent to t*he administrator for approv*al.
   - *Forward to Next Stage:* Upon escalation, the request is sent to the next stage.
   - *Forward to Administrator:* Upon escalation, the request is forwarded to the security lead defined in *Configuration → Support.*
   - *Deactivate; Forward To Next Stage:* Upon escalation, the role assignments for users on the request are deactivated with the validity date is set to the current date. Then, the request is forwarded to the next stage.
   - *Deactivate; Lock, Forward To Next Stage:* Upon escalation, the users on the request are locked in addition to role assignments being deactivated and the request is forwarded to the next stage.
   - *Lock, Forward To Next Stage:* Upon escalation, the users on the requests have role assignments deactivated and the request is forwarded to the next stage.
10. In the *Notification Configuration* pane,
    - Select the person(s) to receive a notification when the request is *Approved.*
    - Select the person(s) to receive a notification when the request is *Escalated.*
11. In the individual tabs for *Approved, Escalation* and *Next Approver* email notifications, specify the content of the Email *Subject* and the email body. Messages are sent according to this schedule.

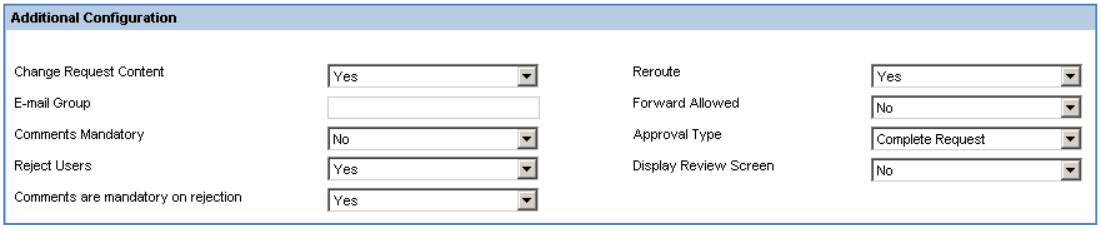
    The *Next Approver* message is sent to the reviewer when the request is ready for their approval.

    The *Approved* message is sent when the current stage's approver submits the review.

    The *Escalation* message is sent if the current stage's approver does not submit the review in the time allowed by the *Request Wait Time.*



12. In the *Additional Configuration* pane, you maintain multiple parameters. The items discussed here are of specific interest during the SOD Review.



- *Change Request Content*
  - *Yes:* Enables the *Approve* and *Remove* buttons during request review. This is required for the Reviewer stage and is optional for the Security stage.
  - *No:* Disables the *Approve* and *Remove* buttons during request review. This is optional for the Security stage. If set to *No*, The reviewer will not be able to specify an action but will only a) take action on direction already noted or b) comment and send the request to another reviewer for update.
- *Email Group:* Obsolete field that is not supported in AC 5.3.
- *Comments Mandatory*
  - *Yes:* Enforces entry of comments regardless of any action taken.
  - *No :* Any entry of a comment is optional.
- *Reject Users*

  The ability to reject users is recommended for the Reviewer stage and is optional for the Security stage.
  - *Yes:* Enables the *Reject User* button during request review.
  - *No :* Disables the *Reject User* button during request review.
- *Comments are Mandatory on Rejection*
  - *Yes:* Requires the reviewer rejecting users to enter a comment regarding the reason for rejection. This may assist the administrator in correcting information for users/roles that are still relevant for review.
  - *No :* Entering a comment is not enforced when a user is rejected from a SOD Review request.
- *Reroute*

  The ability to reroute a request to stages on the request path is controlled by this parameter. This may be used by the Security stage if the Security stage does not allow changes to the requests. Comments may be entered by the Security administrator and the request rerouted to the Reviewer for possible modification after considering the comments.
  - *Yes:* Enables the *Reroute* button during request review.
  - *No:* Disables the *Reroute* button during request review.
- *Forward Allowed*

  Forwarding a SOD Review request is supported only when the entire request is forwarded. To have individual user records reviewed by someone other than the stage reviewer, it is recommended to *Reject* the user and manage the user through the alternate process. See the section *Manage Rejected Users* for more information.
  - *Yes:* This option is not recommended.
  - *No:* This option is recommended.
- *Approval Type*
  - *Complete Request:* All lines of the request are visible at the stage. This is recommended for the Reviewer stage

- *Only Remove Items:* Only the items of the request that have been previously marked for removal will be visible at the stage. This is commonly used for the Security stage. This allows Security to analyze the functions that are marked for removal and determine which roles will be deprovisioned.

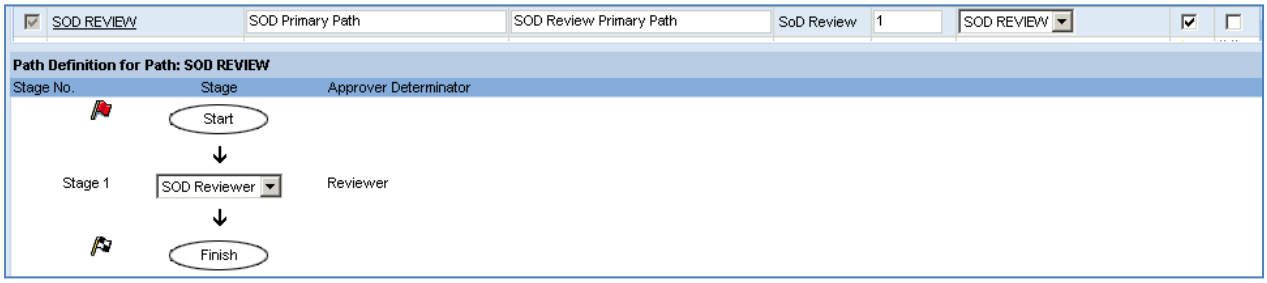
- *Display Review Screen*
  - *Yes:* An approval screen will be shown after the request has been submitted. This approval screen is redundant in the case of the SOD Review.
  - *No:* The last approval screen will be bypassed after the request has been submitted. In the case of the SOD Review requests, the approve or remove action has already been indicated for each line item and this review screen is redundant. This is recommended for SOD Review requests.

13. Specify a value for the *Additional Security Configuration (Approval Reaffirm)* parameter, if necessary. If *Display Review Screen* is set to *No* as suggested, then this field is not editable.
    - *Yes:* The approver must confirm their identity before submission of the review request by entering their password when prompted.
    - *No:* The approver is not prompted to confirm their identity upon submission of the review request.
14. Click *Save* to store the stage definition.

5.2.11.3 Define the Reviewer (Primary) Path

You must define the primary path for SOD Review request approval by reviewers.

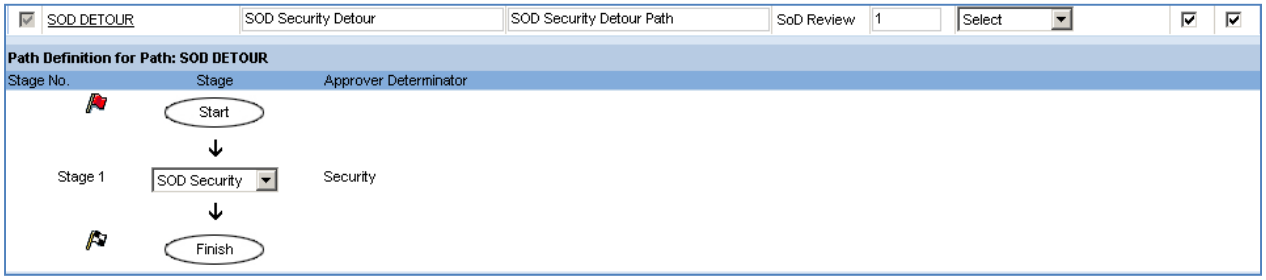
1. Go to *Configuration → Workflow → Path*. The *Workflow Paths* screen appears.
2. Click *Create*. The *Create Path* screen appears.
3. In the Create Path pane, perform the following steps.
   a. In the *Name* field, enter a name for your path. For example, enter *SOD REVIEW'*.
   b. In the *Short Description* field, enter a brief description of the stage.
   c. In the *Description* field, enter a long description of the stage.
   d. In the *Workflow Type* dropdown menu, select *SOD Review*.
   e. In the *Number of Stages* field, enter the number of stages for the primary path. The example workflow has *Number of Stages* equal to *1*.
   f. In the *Initiator* dropdown menu, select the initiator name that you previously created. In this example, the initiator name is *SOD Review.*
   g. Select the *Active* checkbox.
   h. Leave the Detour checkbox unselected.
4. In the *Path Definition* pane, select the stage name for each stage of the path. In the workflow example, *Stage 1* is the *SOD REVIEWER*
5. Click *Save*.



5.2.11.4 Define the Security (Detour) Path

If you are using a detour path for security to evaluate the functions marked for removal during the SOD review, then you will define it following these steps.

1. Go to *Configuration → Workflow → Path*. The *Workflow Paths* screen appears.
2. Click *Create*. The *Create Path* screen appears.
3. In the *Name* field, enter a name for your path. For example, enter '*SOD Detour'*.
4. In the *Short Description* field, enter a brief description for this stage.
5. In the *Description* field, enter a long description for this stage.
6. In the *Workflow Type* dropdown menu, select *SOD Review*.
7. In the *Number of Stages* field, enter *1*.
8. In the *Initiator* dropdown menu, make sure there is no initiator in this field.
9. Select the *Active* checkbox.
10. Select the *Detour* checkbox to indicate that this is a detour path.
11. In the *Path Definition For Path xx* pane, select '*SOD Security'* in the dropdown menu for *Stage 1*.
12. Click *Save*.



5.2.11.5 Maintain Custom Approver Determinator

You can define custom approver determinators (CADs) to be used for additional stages in approval of SOD Review requests. If definition of the process resulted in stages other than the Reviewer (Risk Owner or User's Manager) and Security stages, then define a CAD to be used at this additional stage. The example workflow in this document does not involve a stage utilizing a CAD.

5.2.11.6 Define a Detour

For the example workflow, you will define a detour for line items on the SOD Review request that have been marked for removal.

1. Go to *Configuration → Workflow → Detour/Fork*. The *Workflow Stage Detour* screen appears. The screen defaults to the *Stage Detour* tab.
2. Click *Create*. At the bottom of the table, the entry fields become active.
3. In the *Workflow Type* dropdown menu, select *SOD Review*.
4. In the *Path* dropdown menu, select *SOD Primary Path*.
5. In the *Stage* dropdown menu, select *SOD Reviewer*. In the *Action* dropdown menu, select *Save*.
6. In the *Condition* dropdown menu, select *Items with Remove Action*.
7. In the *Value* dropdown menu, select *Yes*. The *Yes* value indicates that the request will follow the detour if the condition is true.
8. In the *Detour Path* dropdown menu, select *SOD Security Detour*.

5.2.11.7 Define an Email Reminder

You define the email reminder by specifying the time interval allowed to elapse before a reminder notice is sent. You also specify the content of the email.

1. Go to *Configuration → Workflow → Email Reminder*. The *Email Reminder screen* appears.
2. In the *Workflow Type* dropdown menu, select, *SOD Review*.
3. In the *Days* field, enter a number of days from the time that the request first was submitted to the approver's inbox.
4. Click *Save*.
5. Click the *Reminder* tab.
6. In the *Subject* field, enter a reminder statement for the Reviewer.
7. In the *Content* field, you can configure the message for the email body.

> **Tip**
> The email reminder can state that there are a number of requests pending on the reviewer's approval.

8. In the *Email Arguments* dropdown menu, select the argument that identifies the request.
9. In the *Notification Configuration* pane, click *Reviewer*.
10. Repeat the steps above for the *Reminder for Coordinator* tab. Be sure to select *Coordinator* in the *Notification Configuration* pane.
11. Click *Save*.

5.2.12 Configure Service Level (Escalation)

You must define the conditions that will cause an escalation, the action taken for the escalation and the content of the escalation email.

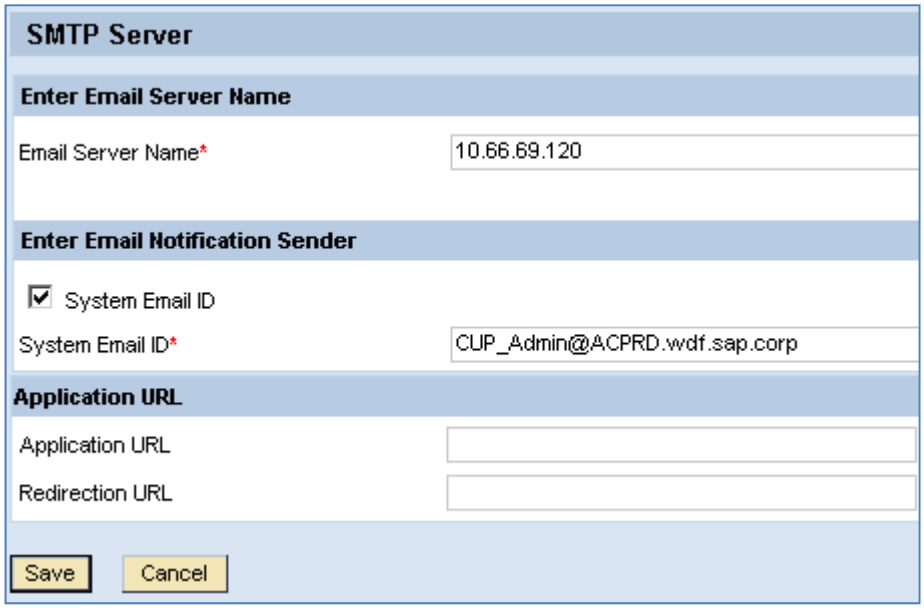
1. Go to the *Configuration → Service Level*
2. Click *Create*. The *Create Service Level* screen appears.
3. In the *Name* field, enter a name for your service level. For example, enter *SOD* Review *Escalation*
4. In the *Short Description* field, enter a brief description for this service level.
5. In the *Description* field, enter a long description for this service level.
6. In the *Workflow Type* dropdown menu, select *SOD Review*.
7. In the *Type* dropdown menu, select either *Formula* or *Fixed.*
   - Formula allows you to specify criteria for the escalation of the request. Fields available to determine the formula are days and attributes (including custom attributes).
   - Fixed allows you to specify a date upon which the request will be escalated. You also specify whether this is a Global Escalation Date. If it is a Global Escalation Date, then the date defined here takes precedence over the escalation date configured at the workflow stage level. When using this option, you must modify the Due Date and Global Escalation Date for new review cycles. If the request generation date is later than the due date, the background jobs for request generation will error. For more information about configuring escalation, see the AC 5.3 Configuration Guide and the AC 5.3 SP06 Supplemental Note 1292484.Complete the definition based on the escalation type chosen.
8. Click *Save*.

5.2.13 Configure an SMTP Server

Compliant User Provisioning uses an SMTP server to send email notifications and reminders to users, requestors, and approvers of requests.

> **Warning**
>
> If this setting is not properly configured, the entire approval process might be jeopardized. If approvers are not getting the email notifications that a request is waiting for their approval, the approvers must log on to Compliant User Provisioning to view the requests waiting for their approval.

1. Navigate to *Configuration → Workflow → SMTP Server*.
   The *SMTP Server* screen appears.
2. In the *Email Server Name* field, enter the name or IP address of the SMTP server that Compliant User Provisioning uses to transmit messages.
3. If a system account rather than the logged on user's account is to be used to send email notices from Access Control, select the *System Email ID* indicator field and identify the system account to be used.
4. Entries in the *Application URL* and *Redirection URL* fields are not required for the SOD Review.
5. Click *Save*.



- Execute the *Email Dispatcher* background job to send email notices from Access Control. For more information, see Setting Up Background Jobs.

5.2.14 Maintain Field Mapping

If you are using an LDAP as the *User Detail Data Source* and SOD Review requests will be approved by users' managers, then you must specify a field mapping for *Manager* so that Access Control can determine the reviewer for workflow. You define this in *Configuration → Field Mapping → LDAP Mapping.*

For more information, see the *Field Mapping* section of the *AC 5.3 Configuration Guide*.

5.2.15 Define a Security Lead

You can specify a group email or approver ID(s) to be used by the security approval stages. On the *Configuration* tab, go to *Approvers → Security Lead* to configure the security lead information.

5.2.16 Maintain Coordinators

You identify a *Coordinator* for each *Reviewer*, regardless of whether the reviewer is a *User's Manager* or a *Risk Owner*. The reviewer and coordinator's names and email addresses will be obtained from the User Detail Data Source using their User ID. Access Control uses the coordinator information to generate reports that can be used while managing the review process.

To maintain individual coordinators manually:

1. Go to *Configuration → User Review → Coordinator.*
2. Choose *Search.*
3. The list of coordinators is shown. Choose Create to identify new coordinators or associate coordinators with additional Reviewers.
4. Enter a *Coordinator ID* and a *Reviewer ID.* (Note that wildcards are not support in the ID fields.)
5. Choose *Save.*

To upload multiple coordinators:

1. Go to *Configuration → User Review → Coordinator.*
2. Choose *Search.*
3. Choose *Download Template* to have the template opened in a spreadsheet.
4. Maintain entries to be uploaded.
5. Save file to your local hard drive .
6. Enter, or browse for, the file name to be uploaded.
7. Choose *Import.*

5.2.17 Define Connectors

For each back-end system to be included in the SOD Review, you must define a connector. The *Connector ID* in CUP must be identical to the *Connector* in RAR so that risk violation information may be retrieved from RAR and imported into CUP for generation of the SOD Review requests.

5.2.18 Maintain UME Security

As of SP06, UME actions for managing the rejected user process are introduced and must be assigned to the appropriate individuals. These actions were provided in the initial data files as of SP06. The general security requirements for Access Control are not discussed here. If you need information on general security, please see the *AC 5.3 Security Guide*.

UME Action	Permission Included
ViewManageRejectionReasons	Provides the ability to configure *Rejection Reasons* to be used in reviews
ViewRejectUsers	Enables the *Reject Users* button in review requests
ViewManageRejections	Provides the ability to view the *Manage Rejections* functionality for the SOD Review process
ManageRejectionsGenerationAction	Provides the ability to generate new requests for rejected users
ManageRejectionsCancelGenerationAction	Provides the ability to cancel the generation of new requests for rejected users

6. Review Execution

6.1 Data Generation in RAR

Once configuration is complete, you perform activities in RAR to generate the data presented in SOD Review requests.

6.1.1 Execute Background Risk Analysis

A full Batch Risk Analysis must be completed for all systems to be included for the SOD Review process. This must be performed while Offline Analysis is enabled so that the risk analysis results will be stored in RAR (in table VIRSA_CC_PRMVL). The web services used by CUP during creation of the SOD Review requests retrieve the data from the RAR offline analysis table.

6.1.2 Purge Usage Information

The usage information in SOD Review requests will have a *From* date dependent on the last purge or the original alert generation period, if no alerts have been purged. The *To* date will be determined by the date of the last job that updated the Management Reports.

If more transaction usage information is stored in RAR than is desired for the SOD Review and UAR Review, then the data should be archived. For example, if your SOD Review process states that the prior twelve months' usage information should be provided in SOD Review requests and RAR has fifteen months available, then the oldest three months information should be purged (archived) in RAR.

It is important to note that usage information purged in RAR is still accessible to RAR from the flat file that is produced but is not accessible by ERM or CUP and is therefore not included in the User Access Review or SOD Review processes.

Purging usage information requires configuration of the location for writing the purge file in RAR *Configuration → Miscellaneous → Alert Log File Name and Location.* For more information on purging usage information, refer to the *AC 5.3 Configuration Guide*.

6.1.3 Generate Alerts

Ensure that the RAR Alert Generation job has been executed if usage information is to be included in the SOD Review requests.

To generate alerts:

1. On the *Configuration* tab, navigate to *Background Job → Alert Generation*.
2. In the *Action Monitoring* pane, select *Generate Action Log*.
3. Select the SAP single or cross systems for which to generate alerts. Only SAP servers that have connectors created appear in the dropdown list.
4. Select all types of alerts to include in the action log.
   - *Conflicting Action*
     Select *Risk ID* equal to *'*'*.
     Select *Risk Level* equal to *All*.
     Select *Consider Mitigated Users*.
   - *Critical Action*
     Select *Risk ID* equal to *'*'*.
     Select *Risk Level* equal to *All*.
     Select *Consider Mitigated Users*.

- *Control Monitoring*

  Select the *Mitigating Control ID* equal to *'*'*.

5. In the *Alert Notification* pane, select the appropriate items according to company policy.
6. Click *Schedule*. The *Schedule Background Job* screen appears.
7. In the Job Name field, enter a name for this job.
8. Select *Immediate Start* or *Delayed Start.* Indicate the date and time to begin.
9. If the job should be performed multiple times, select *Schedule Periodically* and indicate the frequency as well as the *End Date* past which no jobs will execute.
10. Click *Schedule* to accept your input or *Reset* to begin again.

    Upon completion of scheduling, the following message displays: `Background job scheduled successfully, Job ID: XX.` Table VIRSA_CC_ACTUSAGE will be updated with the chosen transaction usage information,

6.2 Create and Distribute SOD Review Requests

Identified below are the steps executed to generate requests for the SOD review and to subsequently generate the workflow tasks for reviewers of the requests. (Please note that generating new requests for users rejected from earlier requests is discussed in the section *Manage Rejected Users*)

Before beginning the user review process, all supporting information for generating requests should be current to ensure accurate workflow of requests. For example, if the Reviewer is configured to be the User's Manager, then the user-to-manager relationships should be current in the detail data source.

Note: If there are users with no manager identified in the *User Detail Data Source* and the *Reviewe*r is defined as the *User's Manager*, then *Admin Review* is required. This allows the administrator to maintain the missing data prior to sending workflow tasks to reviewers.

6.2.1 Execute SOD Review Load Data

The *SOD Review Load Data* task retrieves the SOD risk violation information from RAR and generates the SOD Review requests. Usage information will also be retrieved, if you generated alerts prior to executing the load data task. After successful completion of the load data task, the SOD Review requests are ready for Administrator Review. A subsequent step will send the workflow tasks to reviewers.

As previously discussed, you may retrieve SOD risk violations ignoring or including mitigated risks. The choice depends on the status of your Access Control implementation and your company policy. To perform periodic reaffirmation of previously assigned mitigating controls, you should include mitigated risks.

To create SOD Review requests:

1. Go to *Configuration → Background Jobs.* The *Schedule Task* screen appears.
2. Choose the magnifying glass icon to search for tasks.
3. In the *Search Task* pane, Choose *Go* to display a list of available tasks.
4. In the *Available Tasks for Schedule* pane, select either *SOD Review Load Data with Mitigated Risks* or *SOD Review Load Data without Mitigated Risks.* Choose *OK.*
5. The scheduling screen appears. In the *Description* field, enter a brief description.
6. In the *Schedule Type* dropdown menu, select the time you wish to schedule this job. The corresponding scheduling pane appears.
   a. For *Immediate* schedule type, click *Run*.

b. For jobs that will execute later, enter the *Time* and *Start Date* in the *Recurrence* pane. You can *Activate* the service and/or *Save* the schedule.

> **Tip**
> New SOD Review requests will not be created if open requests remain in Administrator Review. Any SOD Review requests in Administrator Review must be cancelled or have requests sent to reviewers.

6.2.2 Perform Administrator Review

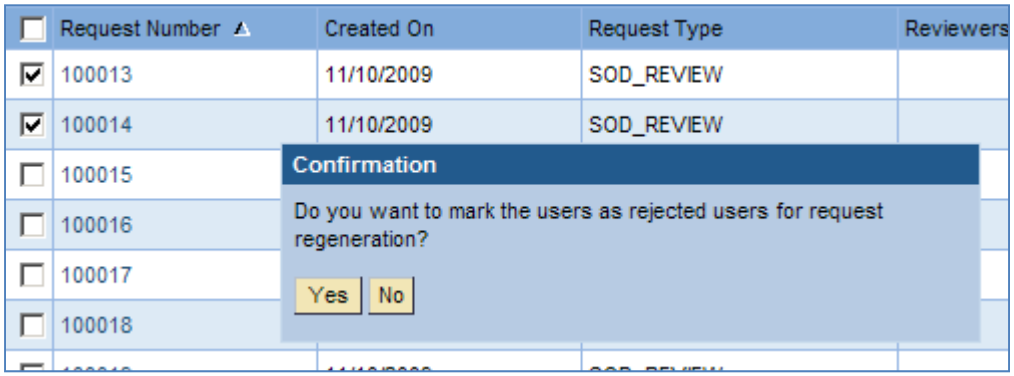
The administrator evaluates the requests to ensure completeness and accuracy of the requests' information prior to sending workflow items to reviewers. If there are few changes to be made, you can manually maintain the reviewer and coordinator information for selected requests.

If many of the requests are incomplete or inaccurate, you:

- Cancel the current *SOD Review* requests.
- Maintain user-to-manager relationships in the *User Details Data Source*.
- Generate new requests.

To perform the admin review:

1. On the *Configuration* tab, navigate to *User Review → Request Review.* The search screen appears.
2. Select *Workflow Type* of *SoD Review.*
3. Choose *Search.*
4. Review the requests' data to confirm accurate reviewer information.
5. To cancel an incorrect request, select a review request number and click the *Cancel Request(s)* button. If you choose to cancel a request, Access Control will ask you to indicate whether the users contained in the request(s) being cancelled should be marked as rejected users.



Yes: The review request is cancelled. All users in the request are considered *Rejected Users* and are available in the *Manage Rejected Users* screen to be regenerated. This is recommended if a small set of requests are to be cancelled and recreated.

No: The review request is cancelled. All users in the request will only be included in another *SOD Review* request upon selection in execution of *SOD Review Load Data* job. This is recommended if all requests are to be cancelled and recreated.

> **Tip**
> If you mistakenly choose to cancel a request and want the request to remain, select an item in the Configuration menu to exit the current menu option.

6.2.3 Execute SOD Review Update Workflow Job

After the *SOD Review Load Data* job has completed and you have performed Admin Review (if appropriate), you execute the *SOD Review Update Workflow* job to push the workflow tasks to the reviewers. In CUP, go to *Configuration → Background Jobs* and select the task *SOD Review Update Workflow.*

To generate workflow tasks for the user review:

1. Go to *Configuration → Background Jobs.* The *Schedule Task* screen appears.
2. Choose the magnifying glass icon to search for tasks.
3. In the *Search Task* pane, Choose *Go* to display a list of available tasks.
4. In the *Available Tasks for Schedule* pane, select *SOD Review Update Workflow.* Choose *OK.*
5. The scheduling screen appears. In the *Description* field, enter a brief description.
6. In the *Schedule Type* dropdown menu, select the time you wish to schedule this job. The corresponding scheduling pane appears.
   a. For *Immediate* schedule type, click *Run*.
   b. For jobs that will execute later, enter the *Time* and *Start Date* in the *Recurrence* pane. You can *Activate* the service and/or *Save* the schedule.

6.2.4 Generate Notifications

E-mail notifications are generated for reviewers with the next execution of the *Email Dispatcher* job. The SOD Review notification emails will contain a hyperlink to the CUP (SOD Review) request.

6.3 Process SOD Review Requests

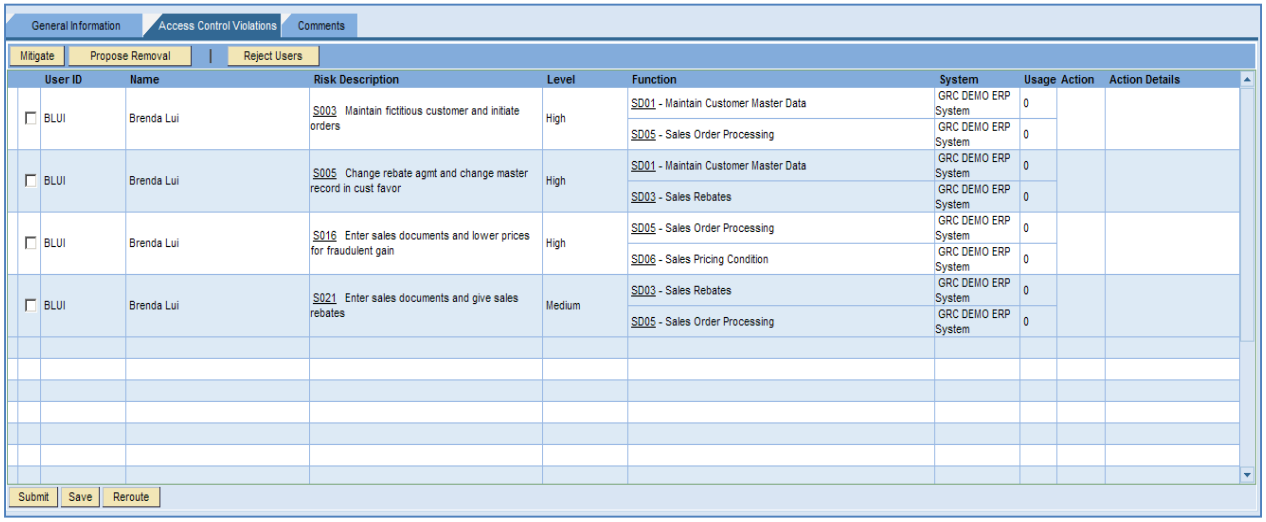
6.3.1 Perform Reviewer Tasks

When the approver logs in to Access Control, the SOD Review requests for his approval will be in the *My Work* tab. The *User Name* column will be blank for SOD Review requests since there may be multiple users on each request.

The *General Information* tab of the SOD Review request will indicate the Reviewer and the Coordinator.

The *Access Control Violations* tab of the request will list the user being reviewed as well as the role and the usage information for the role. You may choose any column header to sort the request lines by that column.

Note: Sorting removes any selections that have not been updated in the *Action* column.



There are multiple actions to be considered by the approver:

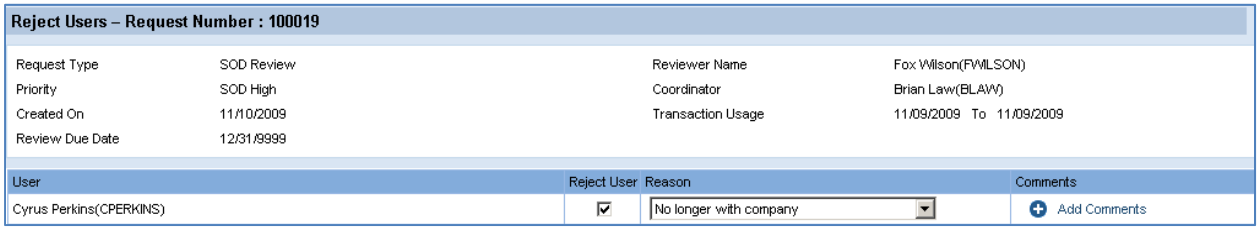
- Rejection of a user where the approver is not the appropriate approver.
- Request for removal of access where the access is inappropriate or the risk violation is not warranted.
- Approval of access which is necessary and the assignment of a mitigating control for remaining risks.

6.3.1.1 Reject User

As of Support Package 06, an approver may reject users for whom they are no longer responsible during SOD Review processing. Once rejected, users are able to be included on new requests. Rejected users are visible in the SOD Review History Report and the User Review Status Report. Whether the approver is the *User's Manager* or the *Risk Owner*, rejection of items from an SOD Review request is for a user. Therefore, rejection of items by a *Risk Owner* with subsequent generation of SOD Review requests for rejected items results in all risk violations for the rejected user being included on a new SOD Review request(s).

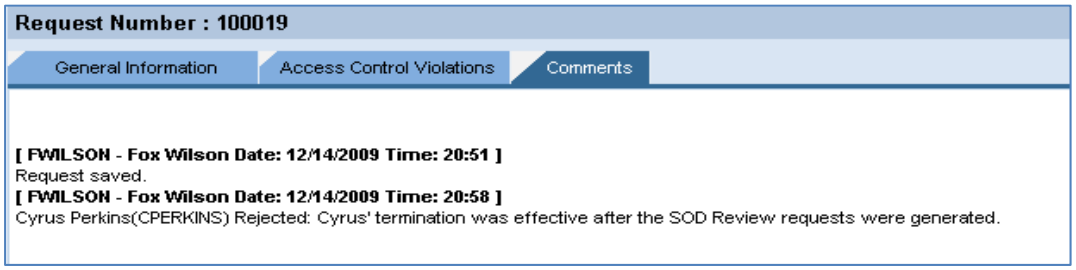
To reject users from SOD Review requests for which you are the approver*:*

1. Go to *My Work → Request for Approval*.
2. Select an *SOD Review* request. Go to the *Access Control Violations* tab.
3. Click the *Reject User(s)* button.
4. The *User* pane appears and displays the list of users.
5. Click the *Reject User* checkbox next to the user you want to reject.
6. Click the *Reason* dropdown box and select a reason.

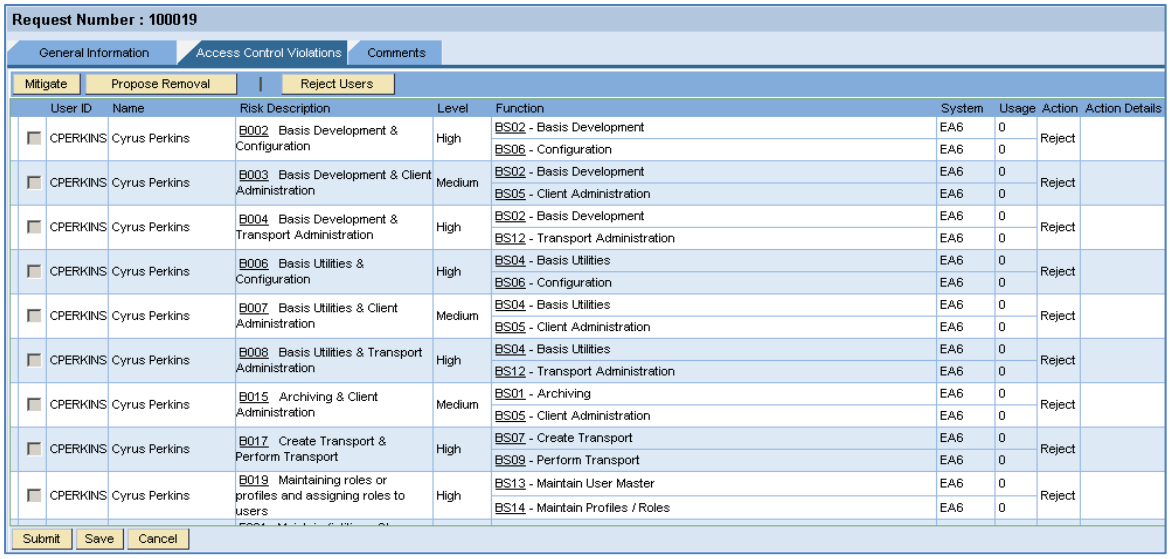


7. If appropriate, choose *Add Comments*, enter a comment, and click *Save*.

   To view previous comments, go to the *Comments* tab. Comments are listed for each rejected user with a time stamp and a reviewer User ID.



The result is that the Action column is populated with Reject for all request items for the chosen user. They are also grayed and inactive. You can return to the Reject User screen and modify rejections prior to submitting the review request. Once you submit the request, the rejected items cannot be modified in a later stage. This applies even if the request is rerouted to another stage.



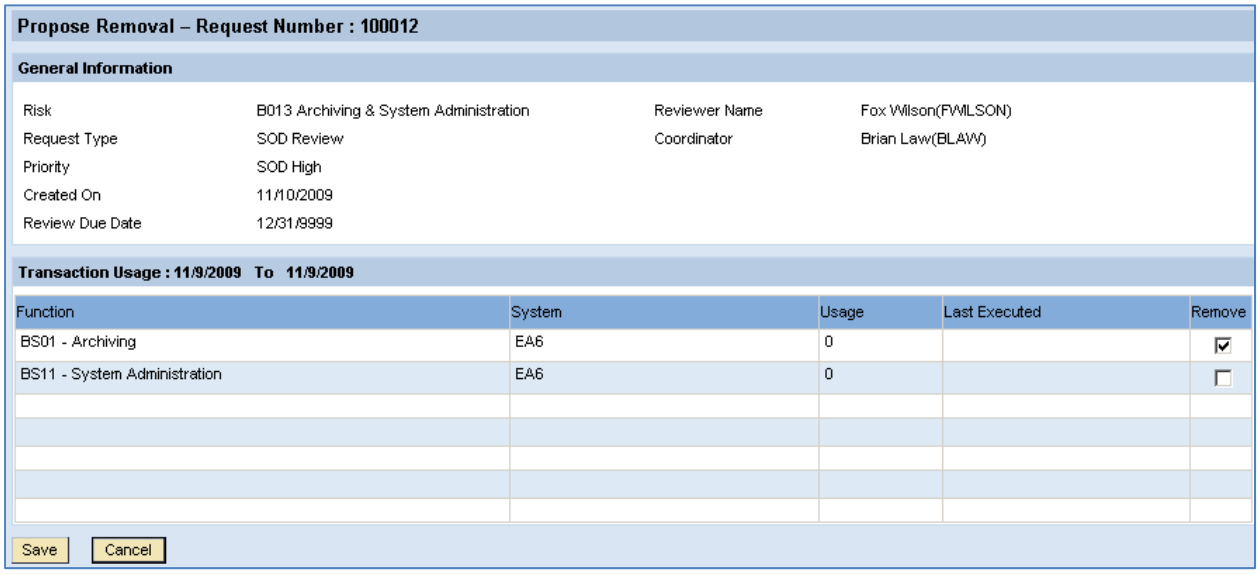
8. On the *Request Number screen*, choose *Save* periodically to save your work while the review is in process
9. Proceed to approve or request removal of functions for each item. Note that rejected items will be available in the *Manage Rejected Users* screen with the status *New* after the request has been submitted.

6.3.1.2 Request Removal of Functions

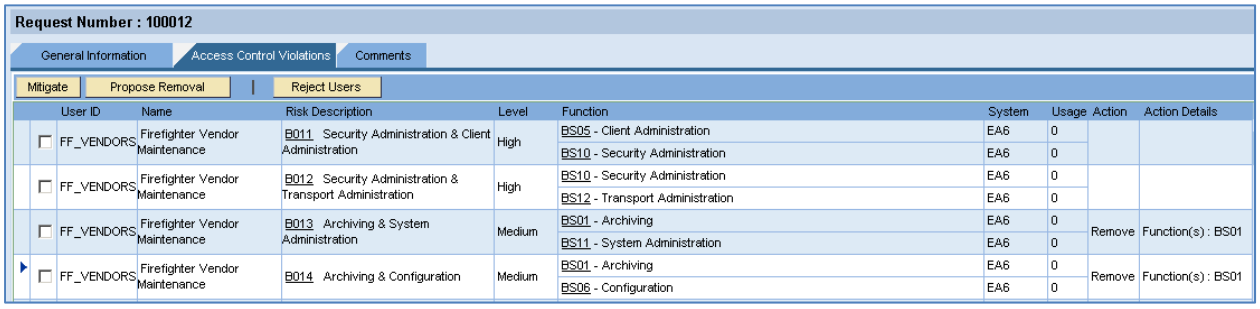
Where access can be removed to eliminate risk violations, the reviewer indicates which function(s) shall be removed.

1. Go to *My Work → Request for Approval*.
2. Select an *SOD Review* request. Go to the *Access Control Violations* tab.
3. Choose a risk violation and choose *Propose Removal.*

4. On the subsequent screen, indicate the function to be removed.



5. Choose *Save.* This causes the *Action* column to be updated. With each update of the action to be taken, the blue triangle denotes the item(s) just updated.



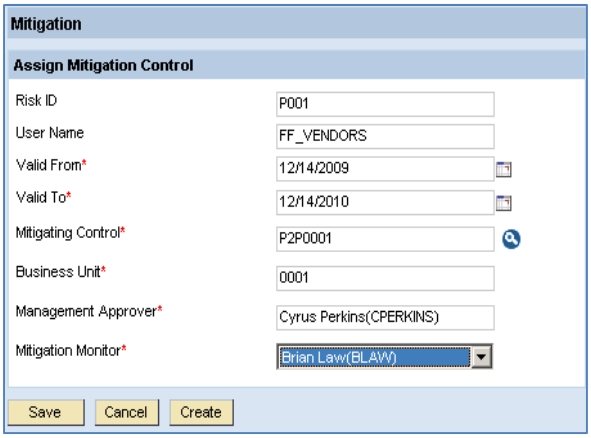
6. On the *Request Number screen*, choose *Save* periodically to ensure work is saved in the request. The request will not be forwarded for the next action until the reviewer chooses *Submit.*

6.3.1.3 Assign Mitigating Controls

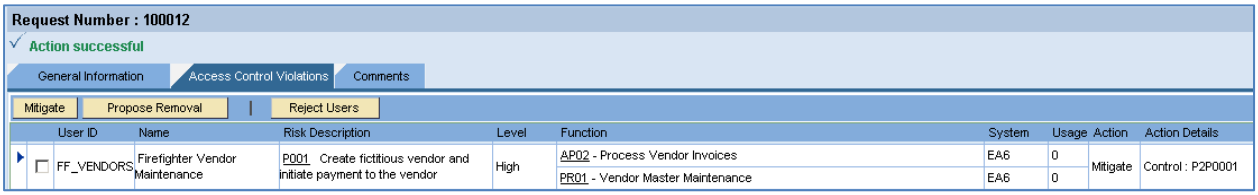
Where access cannot be removed or modified to eliminate risk violations, the reviewer may mitigate the risk by assigning a Mitigating Control.

1. Go to *My Work → Request for Approval*.
2. Select an *SOD Review* request. Go to the *Access Control Violations* tab.
3. Choose a risk violation and choose *Mitigate.*
4. On the subsequent screen:
   4.1 Modify the default validity period, if appropriate.

4.2 Choose the magnifying glass to locate the appropriate *Mitigating Control* defined in RAR. Select the monitor to be assigned.



5. Choose *Save.* This causes the *Action* column to be updated. With each update of the action to be taken, the blue triangle denotes the item(s) just updated.



6.3.1.4 Submit Review

When all roles on the request have been reviewed and each row has been approved, marked for removal or mitigated, the reviewer chooses *Submit* on the *Access Control* Violations tab to complete his work. The request will continue to the next stage.

6.3.2 Manage Rejected Users

As of Support Package 06, the *Manage Rejected Users* process provides authorized users with the following functionality:

- Search for rejected users.
- View search results and sort the results by user.
- Generate review requests.
- Cancel review request generation for those requests that have not been completed.

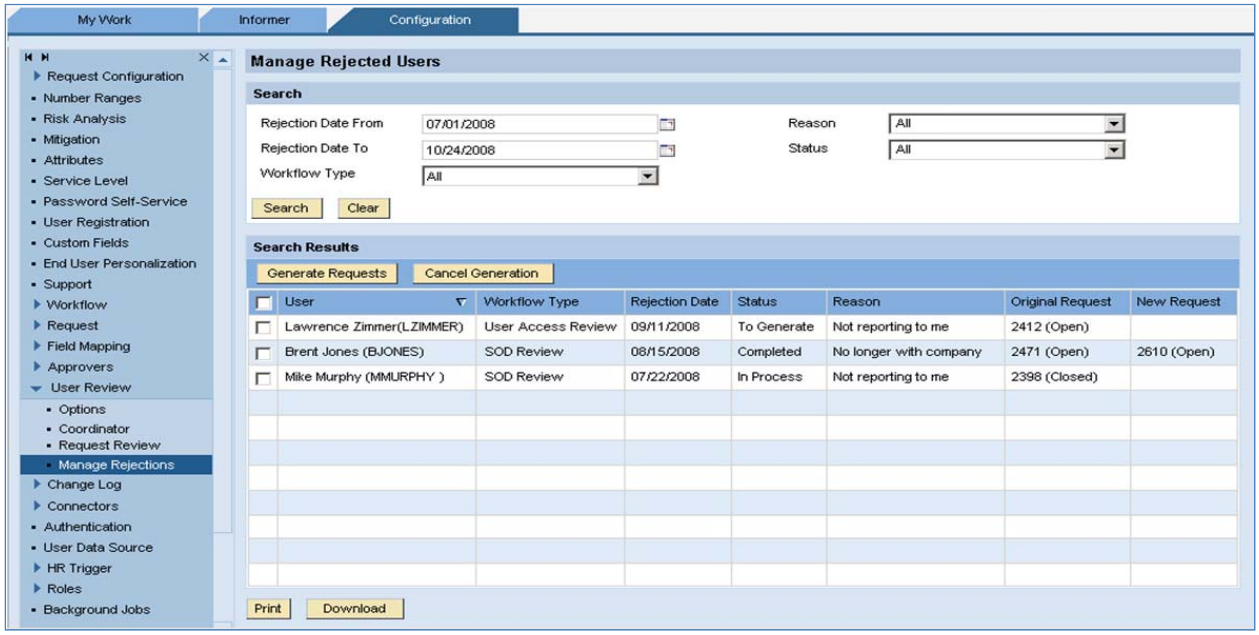
To access the screen, log on to *Configuration → User Review → Manage Rejections.*

6.3.2.1 Search for Rejected Users

You can search using the following fields:

Field	Possible Values	Default Value
Rejection Date From	Any date	Current date
Rejection Date To	Any date	Current date
Note The *Rejection Date* is the date the rejected review request is submitted. If the reviewer rejects a request and only saves the request without submitting it, the user is not available on the screen above. For more information, see *Reviewer Rejects User in Request for Approval.*		
Workflow Type	• SOD Review	All
Reason	Any reason code for rejecting a user.	All
Status	• All • New • To Generate • In Process • Error • Completed	All

The rejected users resulting from the search are displayed.



The following columns are available:

Column	Description
User	You can sort the users by the User IDs.
Workflow Type	This column displays the related workflow type: SOD Review or SOD Review.

Rejection Date	This column displays the date the user is rejected.
Status	The following statuses are available: • **New** These are users that have been rejected by the reviewer and no subsequent action has taken place. To generate new SOD Review requests for these users, they must have their status set as *To* Generate. • **To Generate** The user is marked for inclusion on a new SOD Review request with the next execution of the background request generation job. , x You can click *Cancel Generation* to cancel the request generation since the background request generation job for this user has not started. • **In Process** The background generation job has started but has completed. Regeneration requests with this status cannot be cancelled. • **Error** The generation background job has encountered an error. • **Completed** The generation background job has completed. The new request number is updated.
Reason	This column displays the reason a user was rejected from the request.
Original Request	The column displays the original request number and request status for the rejected user.
New Request	The column displays the new request number and status for the rejected user.

6.3.2.2 Select Rejected Users for SOD Review Request Regeneration

Select user names from the *User* column and click *Generate Requests*. This action marks the user to be included on a new SOD Review request when the *SOD Review Process Rejected* background job is executed.

Recommendation

Before generating requests for the rejected users, make sure the users have the correct reviewer information. This will prevent incorrect information entering the request cycle again.

Example

If the reviewer information is stored in an LDAP data source and is incorrect, it should be updated in the LDAP data source so that new requests are generated with the correct reviewer name.

If the admin review option is set to *Yes*, the administrator can choose to modify the reviewer/coordinator information to correct the reviewer information. As of SP06, a request per user is generated for users without a manager in the data source when the *Reviewer* is set as the *Manager.*

6.3.2.3 Cancel Request Generation for Rejected Users

You can choose to cancel a request generation for users whose request status is *To Generate*. To cancel the request generation for particular users, select users from the *Users* column and click *Cancel Generation*.

Once the request status is *In Process*, the background job has started and the request cannot be cancelled.

6.3.2.4 Generate New Requests for Rejected Users

To generate new requests for marked users:

1. Go to *Configuration → Background Jobs*.
2. Search for and select the task *SOD Review Process Rejected*. Choose *OK*.
3. In the *Description* field, enter a brief description.
4. In the *Schedule Type* dropdown menu, select the appropriate option. .
   a. For immediate execution, select *Immediate,* click *Run*.
   b. For scheduled execution, select *On Date* and specify the date.

6.3.3 Generate Reminders

Reminders are sent as determined by configuration when the SOD Review request approvers do not complete the review by the time specified. No change to the request or users occurs at reminder generation.

6.3.4 Escalate Requests

Escalation will occur when an approver has not completed his review by the time specified in configuration. The escalation may include deactivating a user, and/or forwarding to the next stage.

6.3.5 Perform Administrator Actions

Persons assigned the AE_Admin role can perform many actions for SOD Review requests. These actions include:

- Specify reviewers during Admin Review
- Modify Coordinators
- Cancel requests
- Indicate action to be taken for a user(s) on a SOD Review request (retain or remove access)
- Reject users from SOD Review Requests

6.4 Manage the Review Process: User Review Status Report

The *User Review Status Report* allows you to monitor SOD Review requests to ensure that the process is completed in a timely manner. This report is very useful to coordinators or other persons overseeing the review process. You reach the SOD Review Status Report in CUP by navigating to *Informer → Analysis View → Analytical Reports → User Review Status Report.* (This report was introduced in Support Package 05.)

6.4.1 User Review Status Report Purpose

The status report can be used to monitor the review process. It can be useful to administrators, coordinators, and management. Please note that a stage of a review is not considered complete until the reviewer has submitted the request.

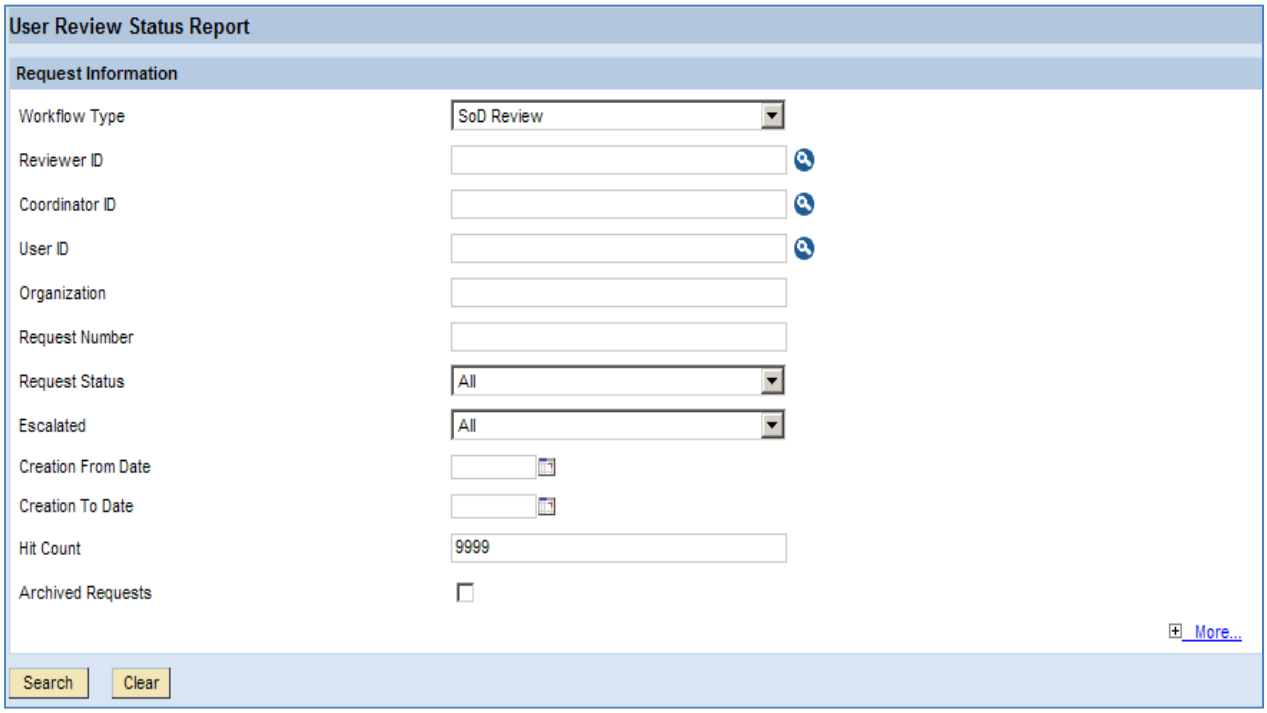
The *SOD Review Status Report*:

- Displays all requests, both complete and incomplete.
- Displays the detailed status of the request by user.
- Can be printed.

6.4.2 Selection Criteria

Shown below is the selection screen for the *User Review Status Report.*

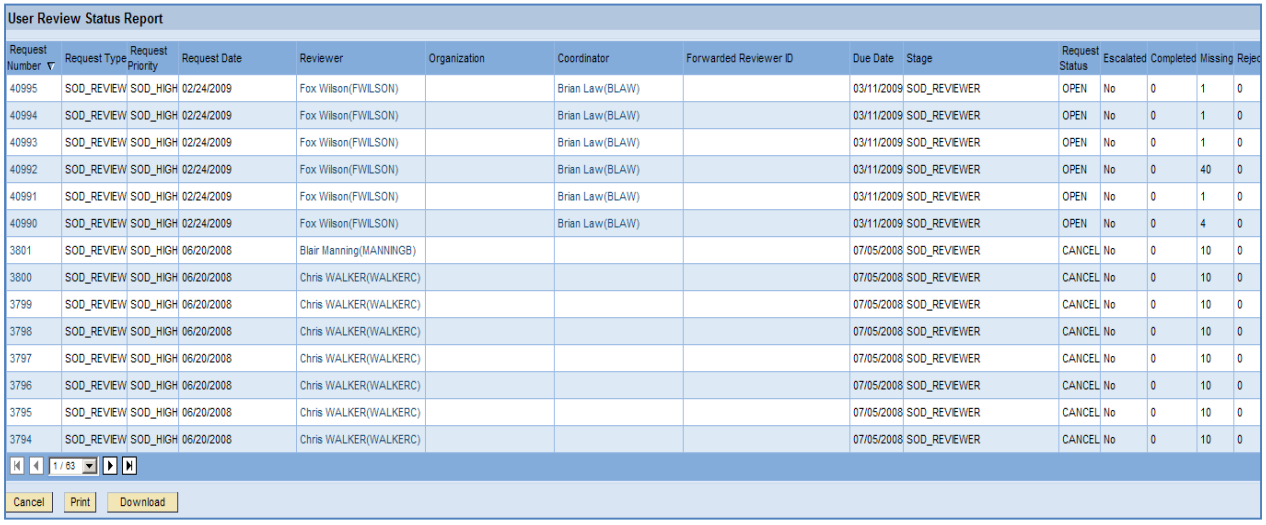
Select *Workflow Type* of *SOD Review.* You may filter results by other criteria, such as coordinator, reviewer, organization, or request status.



Note: Putting a “0” instead of the 9999 Hit Count will return all requests that meet your criteria.

6.4.3 Output

This is an example of the report output screen. You can see the current *Stage*, the number of items *Completed* in the request, *Reviewer,* and other helpful information.



User Review Status Report

Request Number	Request Type	Request Priority	Request Date	Reviewer	Organization	Coordinator	Forwarded Reviewer ID	Due Date	Stage	Request Status	Escalated	Completed	Missing	Rejec
40995	SOD_REVIEW	SOD_HIGH	02/24/2009	Fox Wilson(FWILSON)		Brian Law(BLAW)		03/11/2009	SOD_REVIEWER	OPEN	No	0	1	0
40994	SOD_REVIEW	SOD_HIGH	02/24/2009	Fox Wilson(FWILSON)		Brian Law(BLAW)		03/11/2009	SOD_REVIEWER	OPEN	No	0	1	0
40993	SOD_REVIEW	SOD_HIGH	02/24/2009	Fox Wilson(FWILSON)		Brian Law(BLAW)		03/11/2009	SOD_REVIEWER	OPEN	No	0	1	0
40992	SOD_REVIEW	SOD_HIGH	02/24/2009	Fox Wilson(FWILSON)		Brian Law(BLAW)		03/11/2009	SOD_REVIEWER	OPEN	No	0	40	0
40991	SOD_REVIEW	SOD_HIGH	02/24/2009	Fox Wilson(FWILSON)		Brian Law(BLAW)		03/11/2009	SOD_REVIEWER	OPEN	No	0	1	0
40990	SOD_REVIEW	SOD_HIGH	02/24/2009	Fox Wilson(FWILSON)		Brian Law(BLAW)		03/11/2009	SOD_REVIEWER	OPEN	No	0	4	0
3801	SOD_REVIEW	SOD_HIGH	06/20/2008	Blair Manning(MANNINGB)				07/05/2008	SOD_REVIEWER	CANCEL	No	0	10	0
3800	SOD_REVIEW	SOD_HIGH	06/20/2008	Chris WALKER(WALKERC)				07/05/2008	SOD_REVIEWER	CANCEL	No	0	10	0
3799	SOD_REVIEW	SOD_HIGH	06/20/2008	Chris WALKER(WALKERC)				07/05/2008	SOD_REVIEWER	CANCEL	No	0	10	0
3798	SOD_REVIEW	SOD_HIGH	06/20/2008	Chris WALKER(WALKERC)				07/05/2008	SOD_REVIEWER	CANCEL	No	0	10	0
3797	SOD_REVIEW	SOD_HIGH	06/20/2008	Chris WALKER(WALKERC)				07/05/2008	SOD_REVIEWER	CANCEL	No	0	10	0
3796	SOD_REVIEW	SOD_HIGH	06/20/2008	Chris WALKER(WALKERC)				07/05/2008	SOD_REVIEWER	CANCEL	No	0	10	0
3795	SOD_REVIEW	SOD_HIGH	06/20/2008	Chris WALKER(WALKERC)				07/05/2008	SOD_REVIEWER	CANCEL	No	0	10	0
3794	SOD_REVIEW	SOD_HIGH	06/20/2008	Chris WALKER(WALKERC)				07/05/2008	SOD_REVIEWER	CANCEL	No	0	10	0

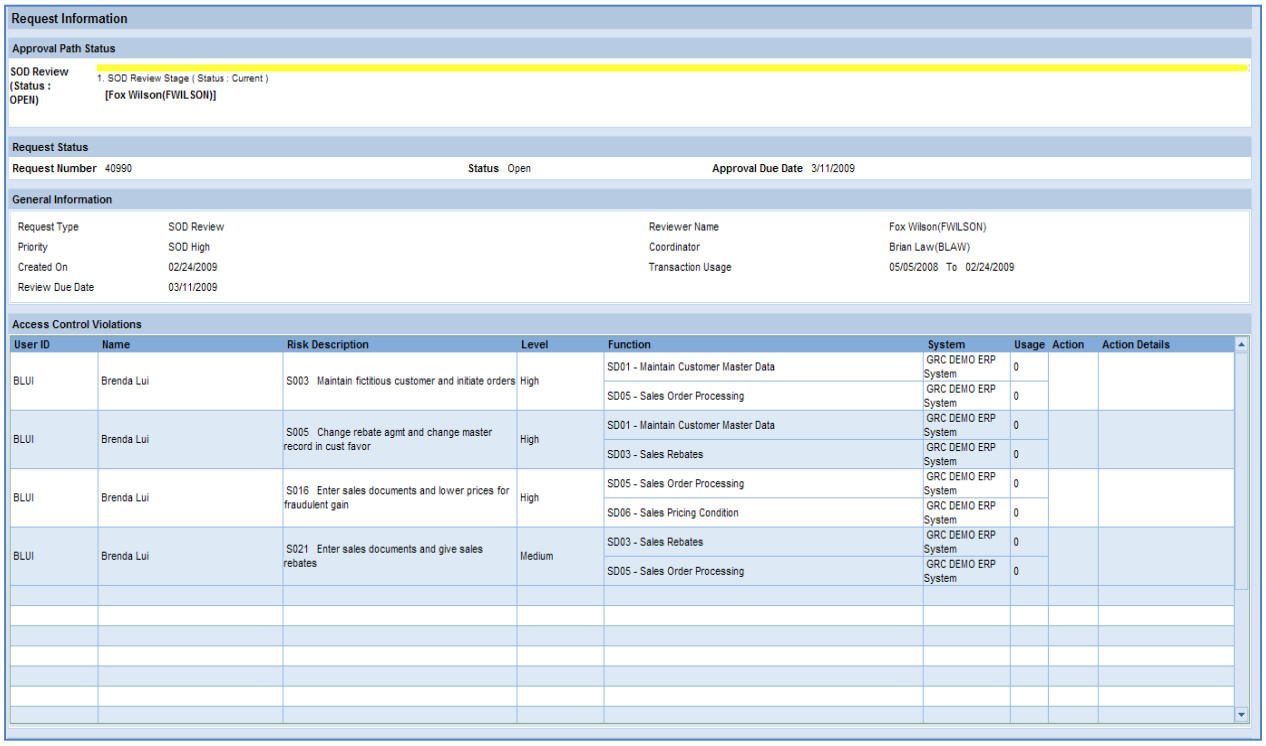
1 / 63

Cancel Print Download

6.4.3.1 Request Details

You can use the hyperlinks for *Request Number* to view the request. Using the scroll bar in the *User Access* pane allows you to scroll through the line items of the request and view the action indicated for each line.

- If the user is rejected and the review request is saved or submitted, all the line items for the user will have *Action* as **Reject**.
- If the request is escalated at any stage of the workflow, all line items in the request will have *Escalated* as **Yes**.



Request Information

Approval Path Status

SOD Review (Status : OPEN)

1. SOD Review Stage (Status : Current)
[Fox Wilson(FWILSON)]

Request Status

Request Number 40990 Status Open Approval Due Date 3/11/2009

General Information

Request Type	SOD Review	Reviewer Name	Fox Wilson(FWILSON)
Priority	SOD High	Coordinator	Brian Law(BLAW)
Created On	02/24/2009	Transaction Usage	05/05/2008 To 02/24/2009
Review Due Date	03/11/2009		

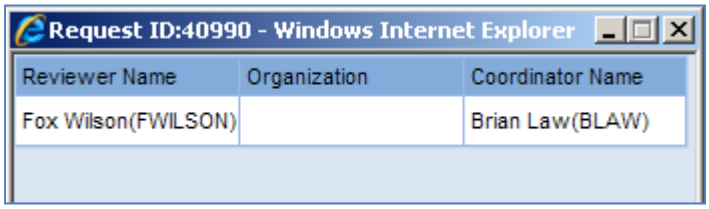
Access Control Violations

User ID	Name	Risk Description	Level	Function	System	Usage	Action	Action Details
BLUI	Brenda Lui	S003 Maintain fictitious customer and initiate orders	High	SD01 - Maintain Customer Master Data	GRC DEMO ERP System	0		
				SD05 - Sales Order Processing	GRC DEMO ERP System	0		
BLUI	Brenda Lui	S005 Change rebate agmt and change master record in cust favor	High	SD01 - Maintain Customer Master Data	GRC DEMO ERP System	0		
				SD03 - Sales Rebates	GRC DEMO ERP System	0		
BLUI	Brenda Lui	S016 Enter sales documents and lower prices for fraudulent gain	High	SD05 - Sales Order Processing	GRC DEMO ERP System	0		
				SD06 - Sales Pricing Condition	GRC DEMO ERP System	0		
BLUI	Brenda Lui	S021 Enter sales documents and give sales rebates	Medium	SD03 - Sales Rebates	GRC DEMO ERP System	0		
				SD05 - Sales Order Processing	GRC DEMO ERP System	0		

Choose *Cancel* to return to the report output.

6.4.3.2 Reviewer Details

You can use the hyperlinks for *Reviewer, Organization,* or *Coordinator to* view details of the reviewer.



7. Audit/Reporting

The SOD Review process provides helpful information for requests or items on requests that are complete. The *SOD Review History Report* shows the actions taken for requests in the user review process. The audit trail of a request shows the detail of the activity taken for the request. Identify the tools available for reporting or auditing the process.

7.1 SOD Review History Report

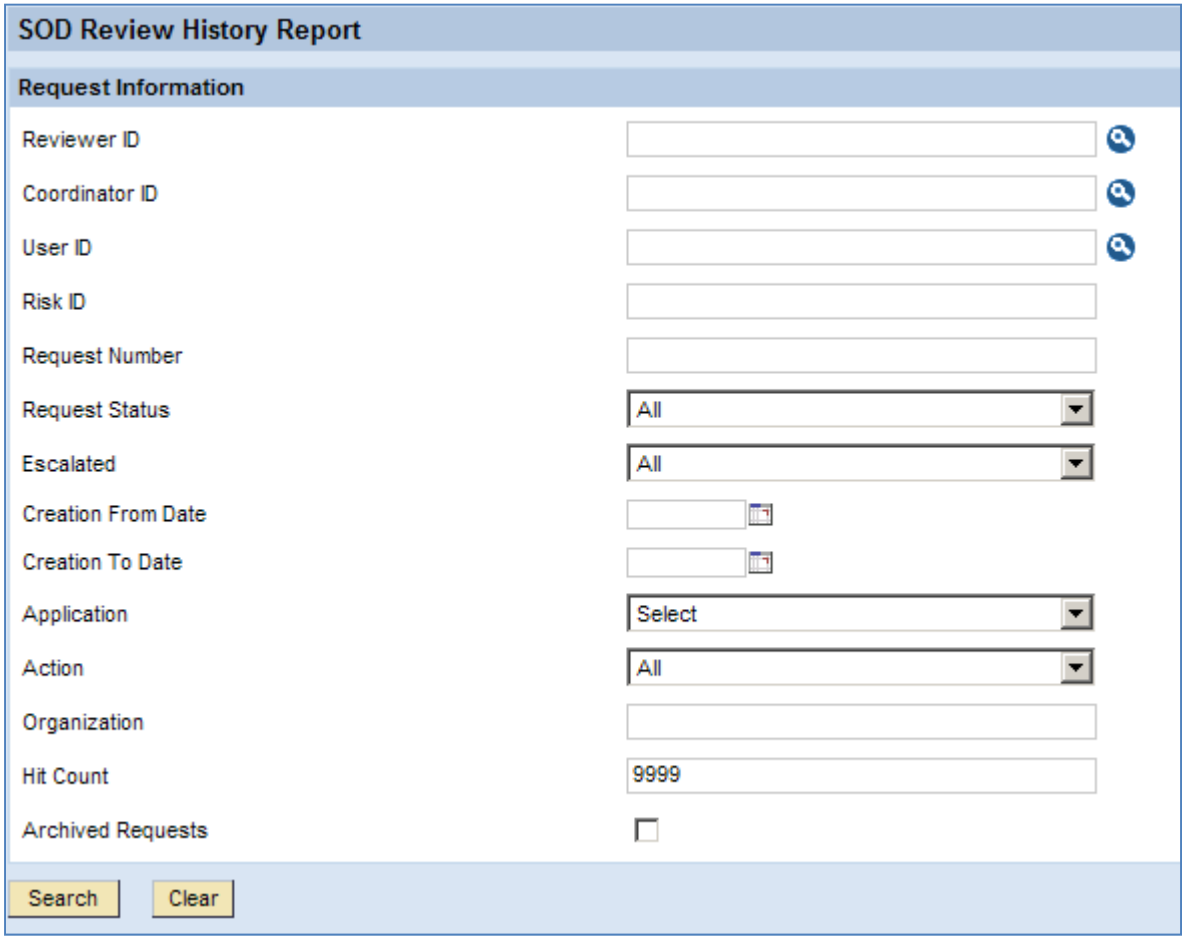
Navigate to *Informer → Analysis View → Analytical Reports → SOD Review History Report.*

7.1.1 Purpose

This report shows the history of activity for SOD Review requests. This is most helpful after a portion of the review process or the entire review process is complete.

7.1.2 Selection Criteria

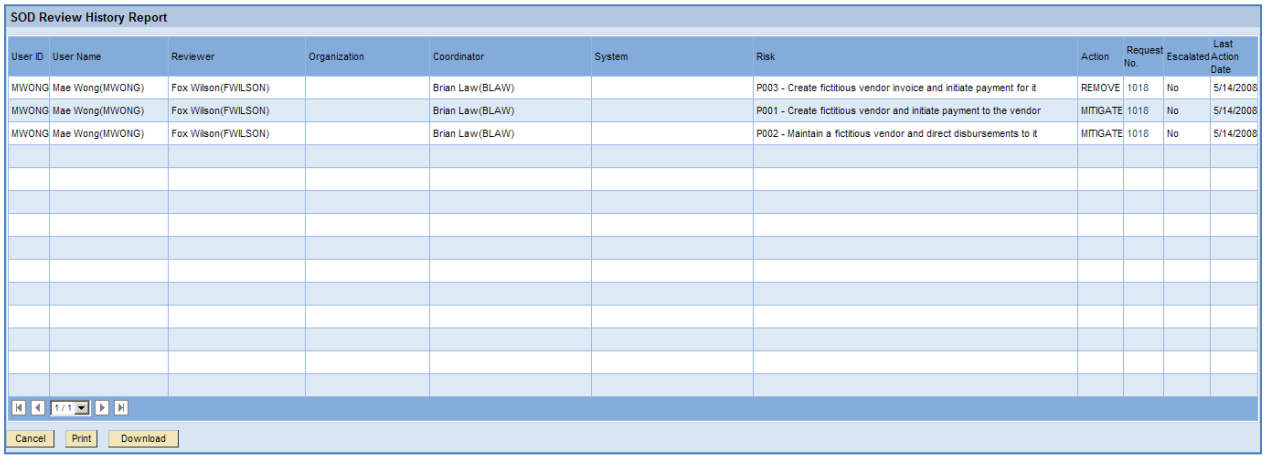
Shown below is the selection screen for the SOD Review History Report. You may filter the requests by multiple criteria, including coordinator and status. You may also filter the report to show only rejected items by choosing the Action of Reject.



Note: Putting a “0” instead of the 9999 Hit Count will produce ALL requests.

7.1.3 Output

Shown below is an example of the report output. You may sort the columns by clicking the column header.



7.1.3.1 Request Details

You can use the hyperlinks for *Request Number* to view the request. Using the scroll bar in the *User Access* pane allows you to scroll through the line items of the request and view the action indicated for each line.

- If the user is rejected and the review request is saved or submitted, all the line items for the user will have *Action* as **Reject**.
- If the request is escalated at any stage of the workflow, all line items in the request will have *Escalated* as **Yes**.

Choose *Cancel* to return to the report output.

7.2 Request Audit Trail

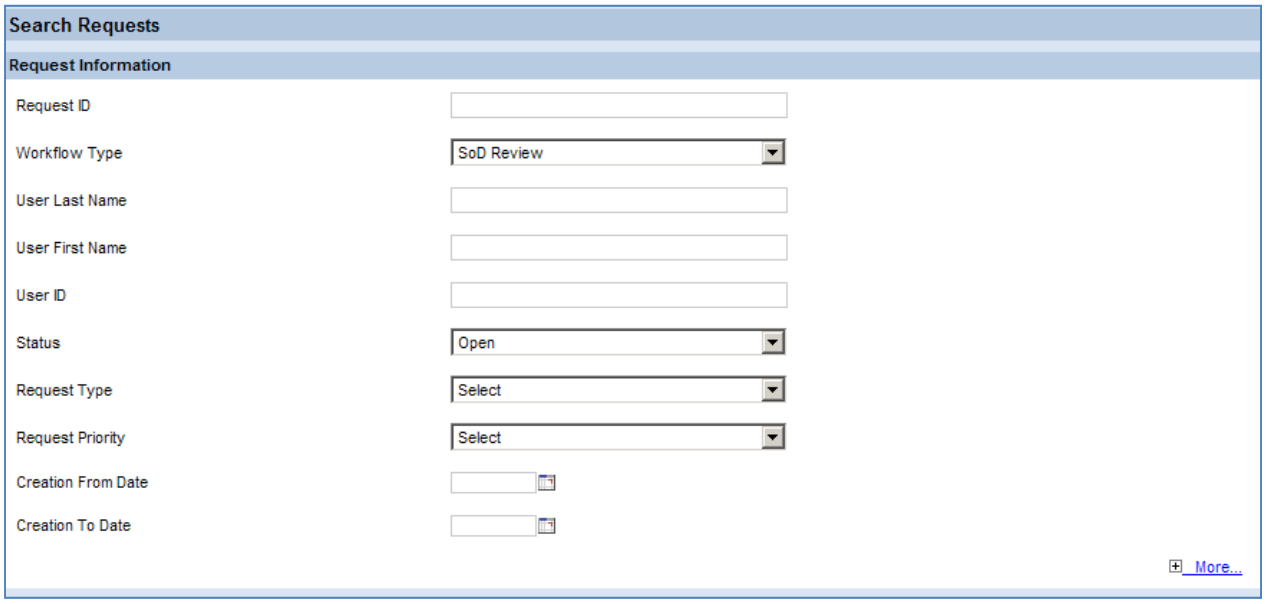
You can view the audit trail of a particular request to see the detailed activity in the life of the request. Navigate to *My Work → Request Audit Trail*

7.2.1 Purpose

This information is very helpful to internal or external auditors. It is also helpful to member of the review team when investigating specific roles or users.

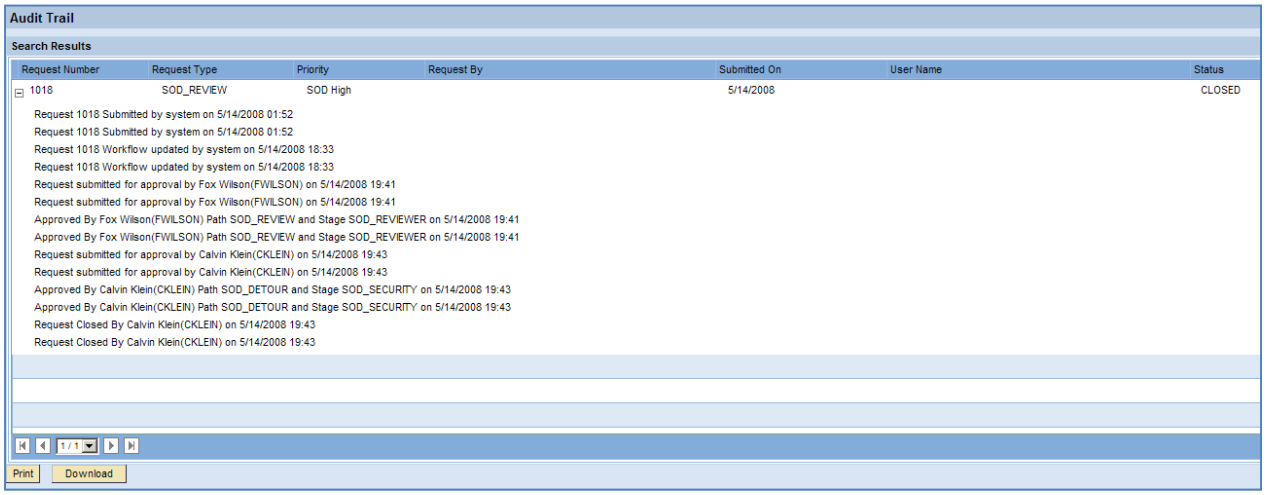
7.2.2 Selection Criteria

Shown below is the selection screen for searching requests. You may enter a specific request ID or choose Workflow Type of SOD Review. You may filter results by other criteria, such as coordinator, reviewer, organization, or request status.



7.2.3 Output

The *Audit Trail* shows the history of the report from request creation through closure. It may be printed or downloaded.



8. Related Content

Access Control 5.3 Configuration Guide

Access Control 5.3 Security Guide

Access Control 5.3 Application Help

Access Control 5.3 SP06 Supplemental Note 1292484

9. Contact Information

Your feedback regarding this document is important to us. Please send comments or corrections to the following email address: GRC_CAO_Access_Control@sap.com.

10.Copyright