USER GUIDE | PUBLIC

2018-11-19

SAP Audit Management

THE BEST RUN

Content

1 SAP Audit Management

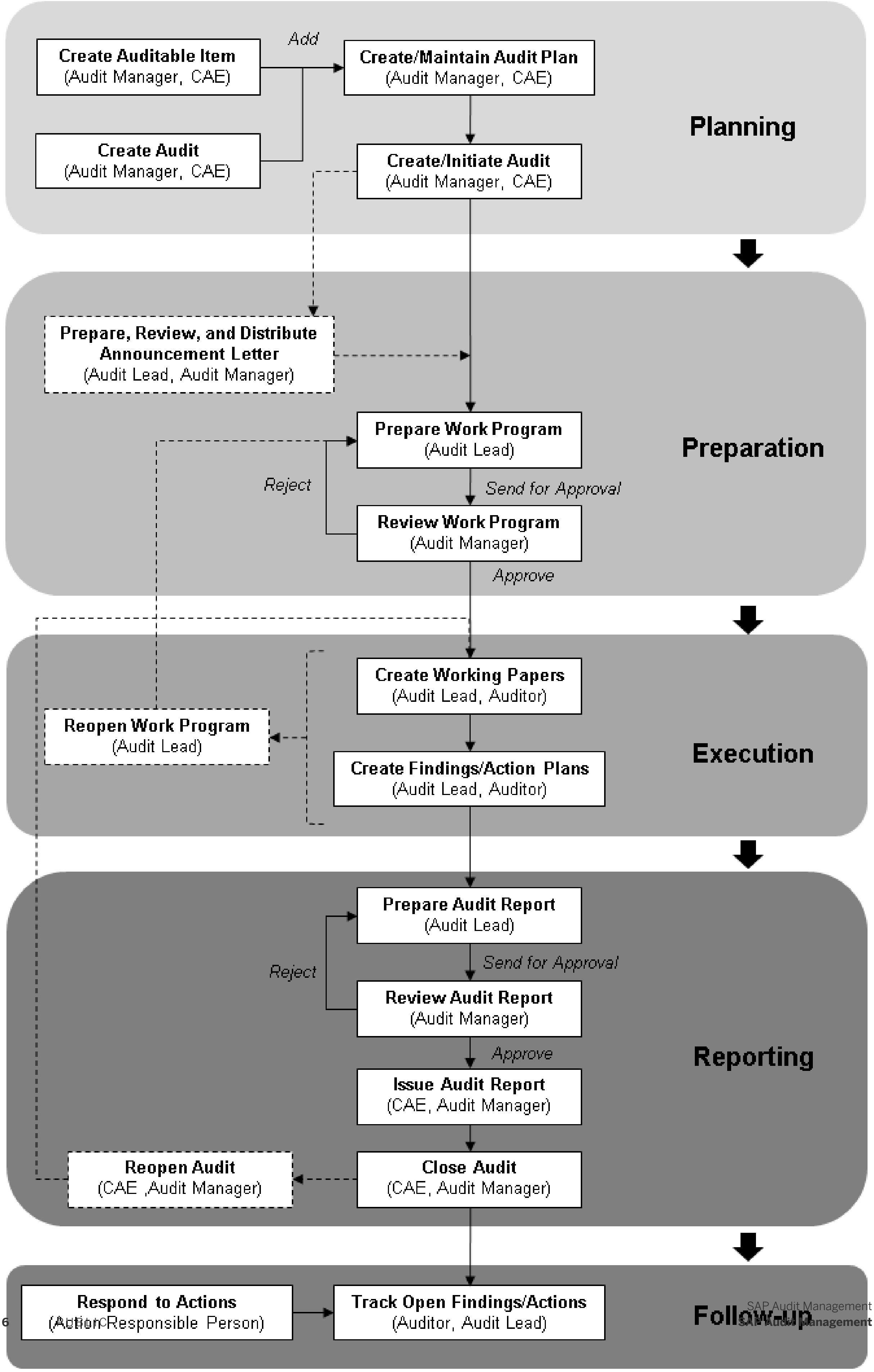
The *SAP Audit Management* solution is part of SAP Assurance and Compliance Software.

Powered by SAP HANA, SAP Audit Management provides a fully mobile enabled, end-to-end audit management solution. The audit department can use it to build audit plans, prepare audits, analyze relevant information, document result, form an audit opinion, communicate results, and monitor progress. The key features of SAP Audit Management include:

- Full mobile-enablement and easy access from multiple devices and platforms
- Full coverage of the audit roadmap; including planning, preparation, execution, report, and follow-up
- Flexible *Audit Universe* that serves as a single source for audits and monitors audit requests globally
- Integration with third-party systems such as SAP Business Integrity Screening and SAP Risk Management
- Powerful working paper management that allows you to create audit documents via drag-and-drop, single-click access to the documents, and management review
- Global monitoring of findings and following up on the progress of actions
- Powerful search function that helps you find the target information through one click
- Clear and intuitive user interface design that improves user experience and boosts efficiency

In SAP Audit Management, the auditing process is divided into five phases: planning, preparation, execution, reporting, and follow-up. Different audit tasks are performed in different phases.

The following figure illustrates the workflow of an audit in SAP Audit Management. Note that the roles only serve as an example of a typical auditing scenario in an organization. You may have different roles for each action depending on your authorization settings.



SAP Audit Management

> i Note
>
> The audit announcement letter approval process is an optional feature depending on the audit status schema configuration.

This documentation is generally structured in accordance with the above five phases. It includes the following sections:

- Setting Up SAP Audit Management [page 11]
  In this section you will find information about roles and back-end transactions in SAP Audit Management.
- Home [page 18]
  Home is the starting point of SAP Audit Management. It gives you an overview of the status and progress of your current tasks, and is a portal to access your tasks.
- Master Data [page 22]
  The master data section provides you with information about risks, controls, dimensions, and organizational units that can be used for risk-based auditing.
- Planning [page 33]
  In the audit planning phase, overall strategies and focus areas are defined for your organization. In this section, you will find the information about *Audit Universe* and audit plans, and the procedures to create auditable items, audits, and audit plans.
- Preparation [page 62]
  In this section, you will find out how to prepare detailed work programs for the assigned audits, how to assign responsible persons to detailed work packages, and how to review the work programs. Optionally, you can also prepare an audit announcement letter and distribute it to the stakeholders.
- Execution [page 74]
  The execution phase is when all the actual field work takes place. Here you will find out how to manage working papers, how to document your audit work, and how to create findings and propose action plans based on your audit evidence.
- Reporting [page 89]
  In the audit reporting phase, audit reports are prepared based on the auditor's work. In this section, you will find the information about the drafting, reviewing, and issuing of audit reports.
- Follow-Up [page 93]
  In this section, you will find information about following up on the findings and action plans resulted from the auditing process.
- Manage Working Papers [page 101]
  In this section, you will find information about how to create, edit, review, and manage versions of audit working papers through the audit lifecycle.
- SAP Audit Management Extensibility Guide
  The *Extensibility Guide* provides advanced information about extending the functionality of SAP Audit Management for you to further explore the potential of the product.
- Data Protection [page 105]

For more information about the terminology used in SAP Audit Management, see http://sapterm.com.

Related Information

SAP Assurance and Compliance Software
SAP Business Integrity Screening

SAP Business Partner Screening

SAP Tax Compliance

2 What's New in SAP Audit Management 1.3 SP01

Release 1.3 SP01 introduces the following new and enhanced features.

New Fiori Apps

Name
Initiate Audits
Prepare Audits
My Ongoing Audits
Track Ongoing Audits
Approve Audit Preparation
Approve Audit Reports
Display Historical Audits

Apart from better user experience, the new Fiori apps also deliver the following new features.

- **Add links as working papers**
  In addition to files, you can now add a link as a working paper.
- **Work program hierarchy**
  The work packages/scopes in a work program are displayed as an intuitive hierarchy.
- **Access to related procedures**
  In a finding, you can see in which procedure(s) this finding was reported and navigate to the procedure(s).
- **Upload a new version of a working paper on its details page**
  You are now able to upload a new version of a working paper on its details page

Enhanced Features

- **Disable automatic risk assignment**
  Previously, when you assign an auditable item to an audit, the risks assigned to the auditable item are automatically assigned to the audit. Now, you can disable the automatic assignment in the Customizing activity *SAP Audit Management* > *Audit Planning* > *Define Audit Types*.
- **Ability to create custom URL field**
  You are now able to create a custom field of type URL.
- **Open homepage search results in Fiori app**
  Use the *Search* bar on the homepage and click on a returned result, the result will be opened in the corresponding Fiori app.

Technical Details

Product Version	SAP Assurance and Compliance Software 1.3 SP01
Application Component	GRC-AUD (SAP Audit Management)
Country Dependency	Valid for all countries
Available as of	November 2018

Related Information

What's New in SAP Assurance and Compliance Software 1.3 SP01
What's New in SAP Assurance and Compliance Software

SAP Audit Management [page 5]

3 Setting Up SAP Audit Management

In the following sections you will find the information you need to set up the application, including authorizations, transactions, language settings, and browser settings:

- Back End Transactions for SAP Audit Management [page 11]
- Roles in SAP Audit Management [page 12]
- Browser Settings [page 17]
- Language Settings [page 17]
- SAP Jam Integration [page 17]

Additional Information

For more technical information, see the *Installation Guide*, *Upgrade Guide*, *Security Guide*, and the *Extensibility Guide* on the SAP Help Portal at http://help.sap.com/audit.

3.1 Back-End Transactions for SAP Audit Management

The following transactions are available in the *SAP Audit Management* menu:

Transaction Name	Transaction Code	Path
Start SAP Audit Management	`/UI2/FLP`	*SAP Menu* > *Audit Management* > *Start SAP Audit Management*
Delete Auditable Items	`GRCAUD_DEL_AUD_ITEM`	*SAP Menu* > *Audit Management* > *Tools* > *Delete Auditable Items*

Data Protection

Menu path: *SAP Menu* > *Audit Management* > *Data Protection*

Transaction Name	Transaction Code	Description
Remove User Names	ACS_DP_ANONYMIZATION	Use this function to remove user names for data that is not going to be archived.
Garbage Collector	ACS_DP_GCO	Use this function to delete unwanted data.
Display Data Protection Logs	ACS_DP_LOG	Use this function to display the application log for data protection activities.
Archive Administration	SARA	Use this function to archive data.
Data Destruction	ILM_DESTRUCTION	Use this function to delete archived data.
Read Access Logging Manager	SRALMANAGER	Use this function to monitor and log read access to sensitive data.

More Information

Close and Delete Auditable Items [page 38]

3.2 Roles in SAP Audit Management

SAP Audit Management has two types of roles: application roles and PFCG roles.

Application Roles

Application roles are the roles you see on the user interface, for example, audit manager, audit lead, and auditor. You can assign these roles to users when you create an audit object.

An application role is only meaningful when it is mapped to a PFCG role, because all user authorizations and menu access derive from the relevant PFCG roles. You can define whether an application role is mandatory, and whether it can be mapped to multiple PFCG roles. You can also specify the identity providers for different application roles in Customizing.

The following application roles are delivered by SAP Audit Management:

Role ID	Role Name	What does this role do?
ACT_RESP	Action Responsible Person	The person who is responsible for the actions proposed in the audit finding.
ADTB_REQ	Auditable Item: Requested By	The person who requested the auditable item in the audit universe.

Role ID	Role Name	What does this role do?
ADTB_RES	Auditable Item: Responsible Person	The person who is responsible for ensuring that the item is audited.
AUDITOR	Auditor	The person who performs auditing in an audit engagement. An auditor: ● Manages working papers ● Creates findings, and action plans
AUD_LEAD	Audit Lead	The audit lead is an auditor who performs the following additional duties: ● Prepares work programs ● Prepares the audit report
AUD_MGR	Audit Manager	The audit manager creates and initiates audits, organizes resources for the audits, and reviews audit work programs and reports.
CAE	Chief Audit Executive	The chief audit executive (CAE) prepares the audit plan for the organization based on risk assessments, overlooks the auditing process, ensures that the audit plan is carried out, and communicates the audit results to the senior management and the board.
EXE_RESP	Executive Responsible	The executive responsible is the person who is responsible for the activity or process to be audited, for example, someone from the management in the auditee's organization.
SCOPE_RESP	Scope Responsible Person	A person assigned to a scope and responsible for the completion of the scope.
TASK_RESP	Task Responsible Person	A task responsible person is an auditor who performs a task, for example, an audit procedure.

PFCG Roles

PFCG roles are back-end roles that provide authorizations and access to menu items. PFCG roles are used in the following two ways:

- PFCG roles can be assigned to users. When you assign a PFCG role to a user, the user can have the authorizations and accesses that are defined in the PFCG role.

- PFCG roles can also be mapped to application roles. When a PFCG role is mapped to an application role, only users who has the same PFCG role can be assigned to this application role during the creation of an audit object.

> Example
>
> PFCG role `SAP_GRCAUD_AUDIT_MANAGER` is mapped to application role `AUD_MGR`. When you create an audit, only the users with the same PFCG role assigned can be selected as the audit manager.
>
> If another PFCG role is also mapped to `AUD_MGR`, then users with this role assigned can also be selected.

In SAP Audit Management, the following standard PFCG roles are provided:

Name	Role	Description
SAP Audit Management: Chief Audit Executive	`SAP_GRCAUD_CAE`	This role allows the user to: • Create, edit, delete, and display organizations • Create, maintain, and release audit plans • Create and initiate audits; delete draft audits • Create and display auditable items • Display work programs, working papers, findings, actions, and audit reports • Obsolete and close findings; complete actions • Display, import, and remove risks in the risk register
SAP Audit Management: Audit Manager	`SAP_GRCAUD_AUDIT_MANAGER`	This role allows the user to: • Display organizations • Maintain audit plans • Create and initiate audits; delete draft audits • Create and display auditable items • Display work programs, working papers, findings, actions, and audit reports • Review, approve or reject work programs, audit announcement letters, and audit reports • Obsolete and close findings; complete actions • Display, import, and remove risks in the risk register

Name	Role	Description
SAP Audit Management: Auditor	`SAP_GRCAUD_AUDITOR`	This role allows the user to: • Display organizations • Display and edit audits • Display auditable items • Create, edit, and display work programs • Create, edit, and delete working papers, findings, actions, and audit reports • Obsolete and close findings; complete actions • Display risks, controls, and dimensions
SAP Audit Management: Action Plan Responsible (Auditee)	`SAP_GRCAUD_ACTION_RESP`	This role allows the user to: • Display action plans • Update status of action plans
SAP Audit Management: Executive Responsible (Auditee)	`SAP_GRCAUD_EXECUTIVE_RESP`	This role allows the user to: • Display, accept, and reject findings • Create, display, change, and update status of action plans
SAP Audit Management: System Administrator	`SAP_GRCAUD_SYSTEM_ADMIN`	This role allows the user to: • Delete auditable items • Import master data • Set reminders for actions and initiating audits
SAP Business Integrity Screening: Manager	`SAP_GRCAUD_FRAUD_INTEGRATION`	This role allows the user to: • Create detection strategies and assign them to tasks • Execute detection strategies, analyze the execution results, and classify alerts
SAP Audit Management - Chief Audit Executive (Fiori Role)	`SAP_BR_ACS_CAE`	This role allows the user to access tiles relevant for CAE in the Fiori Launchpad
SAP Audit Management - Audit Manager (Fiori Role)	`SAP_BR_ACS_AUDIT_MANAGER`	This role allows the user to access tiles relevant for audit manager in the Fiori Launchpad

Name	Role	Description
SAP Audit Management - Auditor (Fiori Role)	SAP_BR_ACS_AUDITOR	This role allows the user to access tiles relevant for auditor in the Fiori Launchpad
SAP Audit Management: Action Plan Responsible (Auditee)-Fiori Role	SAP_BR_ACS_ACTION_RESP	This role allows the user to access tiles relevant for Action Plan Responsible in the Fiori Launchpad
SAP Audit Management: Executive Responsible (Auditee)-Fiori Role	SAP_BR_ACS_EXECUTIVE_RESP	This role allows the user to access tiles relevant for Executive Responsible in the Fiori Launchpad
SAP Audit Management - Integration with SAP Business Integrity Screening (Fiori Role)	SAP_BR_ACS_AUDIT_INT_FRAUD	This role allows the user to access the SAP Business Integrity Screening integration tiles in the Fiori Launchpad

> i Note
>
> The above PFCG roles contain all authorizations and menu entries that are available for SAP Audit Management. This list should only be used as a template. For use in a production system, you must create your custom roles based on these roles, and modify the authorizations and menu entries according to your requirements.

To enable users to send e-mail notifications of audit activities, the following background processing authorization must be maintained for the relevant PFCG roles:

Authorization Object	Field	Value
S_BTCH_ADM	BTCADMIN	Y
S_BTCH_JOB	JOBACTION	RELE
	JOBGROUP	' '

Alternatively, you can also make a copy of standard role SAP_GRCAUD_FRAUD_INTEGRATION and assign it to your user. This role already contains the above required authorization.

For more information about PFCG roles, see the *Security Guide* at http://help.sap.com/audit.

More Information

For more information about how to maintain application roles and role mappings, see the Customizing activities and their documents under *PFCG* > *SAP Audit Management* > *Basic Settings* > *Role Settings*.

3.3 Browser Settings

Using a Logon Screen – Internet Explorer

If you always want to use the logon screen in the browser, you have to choose the following setting for the *Internet Options*. On tab *Security* choose *Custom level...* and disable *Don't prompt for client certificate selection when only one certificate exists*.

Follow Up Tasks After Importing a Transport – All Browsers (Optional)

The browser cache is deleted automatically and periodically. However, if you want, you can run the report `/UI5/APP_INDEX_CALCULATE` to perform an immediate refresh.

3.4 Language Settings

When you start the application, the language that is displayed depends on the following:

- If you select the language on the logon screen, your selection is transferred to the back end with the URL parameter.
- If you use single sign-on (SSO), the language of the browser settings is transferred to the back end.

> i Note
>
> The language settings defined in the *User Maintenance* (transaction `SU01`) in the back end has no influence on the application.

If a text is not available in the logon language, the corresponding text in a fallback language is displayed. Usually the fallback language is English, but in some functions, the "secondary language" defined in the application server is used. To achieve uniform behavior, SAP recommends using English as the secondary language.

3.5 SAP Jam Integration

The application offers an optional integration of SAP Jam, the SAP tool for collaborative work and coordination.

For help with using SAP Jam for collaboration, see http://help.sap.com/jam.

SAP Jam must be added to the SAP Fiori launchpad. If you do not find SAP Jam in your *Home* screen, then see *Adding SAP Jam to the SAP Fiori Launchpad* in the *Installation Guide* or *Upgrade Guide*, at http://help.sap.com/audit.

4 Home

The home page is the starting point of the application. It is based on the SAP Fiori launchpad and can be called using transaction `/UI2/FLP`.

The launchpad opens a home page that contains predefined content, divided into groups. Each group contains tiles that represent business applications. Clicking or tapping a tile launches the underlying application.

The following functions are available on the home page:

- **Personalization**
  The group *My Home* is, by default, the first group on your home page. Other groups may also be visible to you, as defined by your administrator.
  You can personalize the application home page by selecting *Edit Home Page*. Once you do, you can add groups and tiles. As well, you can rearrange existing tiles by dragging them to a new location in a group or moving them to another group.
  Choose *Settings* to display the user account, or to change the appearance or language and regional settings of your screen.
  Choose *App Finder* to search the catalogs for all available tiles.
- **Search**
  With the search, you can find predefined objects, such as detection strategies, alerts, events and documents in alerts.
  You can use the search as follows:

Your Input	Symbol	Result
shares warrants	None	Finds results that contain both the word “shares” and the word “warrants”.
shares OR warrants	OR	Finds results that contain either the word “shares” or the word “warrants”.
shares-warrants	-	Finds results that contain the word “shares” but not the word “warrants”.
warr*	*	Finds results containing words that start with “warr”, for example “warrants”, “warranty”, and “warranted”.
“with best regards”	“”	Finds results that contain the exact phrase “with best regards”.

> i Note
>
> If you can't find the expected results try again using *, for example *12345 or *john*.
>
> The search is not case-sensitive.

In SAP Audit Management, the following objects can be searched using the search from the Fiori launchpad:

- Auditable items
- Audits
- Findings and actions

- Working papers, reports, announcement letters, and attachments
- Risks and controls (latest version)
- Dimensions

Available Tiles

See Available Apps [page 19]

More Information

For more information about using the SAP Fiori launchpad, enter the keyword **`Using the Launchpad`** in the documentation of *User Interface Add-On for SAP NetWeaver* under http://help.sap.com.

4.1 Available Apps

SAP Audit Management 1.3 SP01 provides the following apps, also known as tiles. The apps users have access to are different depending on their roles.

App	Main activities
Approve Audit Report Approve Audit Report (Fiori)	Review and approve audit reports
Approve Audit Preparation Approve Audit Preparation (Fiori)	Review and approve audit announcement letters Review and approve work programs
Audit Universe	Create and maintain auditable items
Controls	Create and maintain controls
Create Auditable Item	Create auditable items
Manage Audit Plans (Fiori)	Plan audit work
Create Audit	Create new audits
Dimensions	Create and maintain dimensions
Display Historical Audits Display Historical Audits (Fiori)	Display historical audits Reopen audits
Display Historical Action Plans Display Historical Action Plans (Fiori)	Display historical actions Reopen actions

App	Main activities
Display Historical Findings (Fiori)	Display and reopen historical findings
Issue Audit Reports	Issue audit reports
Initiate Audit Initiate Audit (Fiori)	Assign audit team members Edit audit details Initiate or delete audits
My Ongoing Audits My Ongoing Audits (Fiori)	Create findings and action plans Generate audit reports Reopen work program
My Profile	Maintain user skills
My Recent Objects	Each link takes you to the individual object screen
Organizations	Add, display, and edit organizational units
Prepare Audits Prepare Audits (Fiori)	Generate audit announcement letters Prepare work programs
Record Time (Fiori)	Record time spent on audit activities
Resource Management	View auditor availability Maintain audit teams
Risk Register	Create and maintain risks
Track Ongoing Audits Track Ongoing Audits (Fiori)	Track ongoing audits
Track Open Action Plans Track Open Action Plans (Fiori)	Track open action plans Change action status Escalate actions
Track Open Findings Track Open Findings (Fiori)	Monitor and change status of open findings Create follow-up action plans
SAP Jam	Shows notifications from SAP Jam on your *Home* screen
Legacy App: Create Audit Plan	Create draft audit plans
Legacy App: Maintain Audit Plans	Maintain draft and reopened audit plan Create new audits in an audit plan

App	Main activities
Legacy App: Display Released Audit Plan	Display released audit plans Copy new audit plans from released audit plans
Legacy App: Display Archived Audit Plans	Display archived audit plans

5 Master Data

In this section, you will find information about the master data in SAP Audit Management, such as risks, controls, and dimensions. The master data provides the audit team with basic information about the organization. This information can be used to create risk-based audit plans.

Related Information

Organizations [page 22]
Risk Register [page 24]
Controls [page 27]
Dimensions [page 29]
Importing Master Data [page 30]
Working with Spreadsheet Templates [page 32]

5.1 Organizations

The *Organizations* tile allows you to view the organizational units in SAP Audit Management. Organizations are displayed in a hierarchical structure. You can expand an organization unit by clicking the + (*Expand Node*) icon. An organizational unit has the following basic information:

- Title: The name of the organizational unit.
- ID: An 8 or 10-digit number that serves as an identifier. The ID is unique to organizational units within the same organization type. When you create a new organizational unit, the ID is generated automatically by the system. You can maintain the number range for generating IDs in Customizing activity *Maintain Number Range for Organizational Units*.
- Description: Description of the organizational unit.
- Type: Organization type.
- Group: Organization group. Organization groups are defined in Customizing activity *Define Organization Groups*.

On the *Risks* tab, you can also find all the risks relevant to this organizational unit.

Organizational units can be created in or imported to the SAP Audit Management system.

For more information about creating, editing, and deleting organizational units, see Creating, Editing, and Deleting Organization Units [page 23].

For more information about importing organizational units from an external system, see Importing Master Data [page 30].

5.1.1 Creating, Editing, and Deleting Organizational Units

Procedure

Follow the procedure below to create a new organizational unit:

1. In the *Organizations* tile, choose *Add* > *Root Organization* to create an organizational unit at the root level. If you want to create a child organization, select an existing organizational unit and choose *Add* > *Child Organization*.
2. On the popup window, enter the following information:

Field	Optional/Required	Description
Title	Required	Title of the organizational unit.
Description	Optional	Description of the organizational unit.
Type	Required	You do not need to enter this field. The default type *Organization* is used.
Group	Required	Choose a group for the organizational unit. You are not allowed to edit this field if you create a child organization. The group of the parent organization is used by default.

3. When you finish, choose *OK* to save the organizational unit.

You can click on the organizational unit to display the detailed information. On the display screen, you can edit or delete the organizational unit.

> i Note
>
> You cannot delete an organizational unit if it has child organizations, or if it has another object assigned.
>
> Organization group must be changed on the root level. Change of group is effective for all child organizations.

You can assign risks and auditable items to an organization. For more information, see Risk Register [page 24]and Creating and Editing Auditable Items [page 35].

More Information

Organizations [page 22]

5.2 Risk Register

The risk register is a central repository for identified risks used in risk-based auditing. In the risk register, risks are categorized by different views. SAP Audit Management has the following default views:

- *Internal Audit* (IA): Risks in this view can be assigned to auditable items and audits for auditing; when you create an audit plan, the risks are also visible on the *Risks* tab.
- *Risk Management* (RM): This view is used to store imported risks from SAP GRC systems.

You can add new views via Customizing activity *Maintain Views for Risks and Controls*.

You can switch from one view to another to display the risks under the view. You can import risks between views, provided that you have the corresponding authorization to access the view and to display risks. For more information, see the documentation for authorization object AUD_VIEW.

In the risk register, you can find the following basic information and risk analysis information on the *Info* tab and on the *Analysis* tab:

Field	Description
Status	Possible risk statuses are *Draft* and *Active*.
ID	The risk ID is automatically generated by the system.
Title	Title of the risk
Organization	Name of the organization to which the risk is assigned
Risk Type	A type assigned to the risk when created
Description	A description of the risk imported from the source system
Validity	Validity dates of the risk
Source System Type	The type of the source system
Source System	Name of source system from which the risk is imported
Source Object	The ID of the risk object in the source system
Last Updated	Information of the last update
Likelihood Level	The likelihood level indicates the probability of the risk.
Impact Level	The impact level is a measure of the effect brought to an enterprise or an organization by the risk.
Risk Level	The risk level is a combined measure that reflects both the impact and likelihood level of the risk.
Analyzed By	The person who performed the latest risk analysis at the time of import

When a risk is assigned to an auditable item, you can also find the information on the *Auditable Items* tab.

The *KRIs* tab allows you to create and modify key risk indicators for the risk. For more information, see Key Risk Indicators (KRIs) [page 26].

You define likelihood levels, impact levels, and risk levels in Customizing activities under *SAP Audit Management* › *Basic Settings* .

Creating Risks

During audit, you might find that there are unidentified risks or that the current risks are insufficient in an organization. The *Risk Register* allows you to propose new risks to the auditee. You can only create risks under the *Internal Audit* view. To do so:

1. Go to the *Risk Register* and navigate to the *Internal Audit* view.
2. Choose *Create* and do the following:
    - Enter the title of the risk
    - Select an organization to assign the risk to
    - Enter the description of the risk
    - Select a risk type
    - Enter the valid dates of the risk
    - Select the risk status

    > **i Note**
    >
    > Possible risk statuses are *Draft* and *Active*. Only active risks can be assigned to auditable items and audit plans for risk-based auditing.
3. When you finish, save the entry.

Mass Upload of Risks

You can upload sets of risks using spreadsheet to mass define risks that you have already created elsewhere.

On the *Risk Register* screen, click *Download Template*. When the download is complete, open the template and enter the required information. Save and upload the completed spreadsheet.

For more information about using the template, see Working with Spreadsheet Templates [page 32].

Creating risk analysis

Risk analysis results are imported along with risks and displayed on the *Analysis* tab. By default, the most recent analysis result is displayed. If no analysis exists for a risk or you want to create a new analysis, you can also do so by choosing the *Analyze* button. On the *Analyze Risk* screen, choose the likelihood level, impact level, and risk level for the inherent risk and the residual risk, and save the analysis.

Assigning controls to risks

On the *Controls* tab, you can add or remove any number of controls from the *Internal Control* view to the risk as responses. When you add a control to a risk, the risk also appears on the *Risk* tab of the control.

Risks are time-dependent

Risks are time-dependent. That means the risk information you see in the risk register is the information the risk had at the time of the last import. Each time a risk is imported from an external system or from another view, the risk is updated with the latest information. A risk might have different information under different views.

When you open a risk from the *Risks* tab of a draft audit plan or an auditable item, the information is synchronous with that of the risks in the *Internal Audit* view. If the risks are updated in the *Internal Audit* view, the latest information is also there in the *Risks* tab of the audit plan or auditable item.

However, when you create an audit based on an auditable item and you assign the risk under the auditable item to the audit, the risk information under this audit is always the same as it is at the time of the assignment. Similarly, when you release an audit plan, all risk information is frozen at the time of the release.

Risk-based auditing

You can use the risks under the *Internal Audit* (`IA`) view for risk-based auditing by assigning them to auditable items and audits, and then including the auditable items and audits in an audit plan. For more information, see Risk Coverage in an Audit Plan [page 43].

5.2.1 Key Risk Indicators (KRIs)

You can use key risk indicators (KRIs) to analyze a risk from different aspects. A KRI allows you to use numeric scores to evaluate the risk.

Creating, Editing, and Deleting KRIs

> i Note
>
> You must maintain the number range before you create a KRI. For more information, see the Customizing activity *Maintain Number Range for KRIs*.

To create a new KRI, go to the *KRIs* tab, choose the + (*Add*) button, enter a title and a description, and choose *OK*.

On the KRI display page, choose edit to modify the title, description, and the KRI value. You can also delete the KRI by choosing the *Delete* button.

More Information

Risk Register [page 24]

5.2.2 Proposing Risks

As an audit manager, you have the option to have new risks created in the SAP Audit Management system proposed to the SAP Risk Management system. You can find the proposed risks in *Proposed Risks and Risk Escalations* in Risk Management.

To propose a risk, go to *Risk Register*, select a risk you created in Audit Management under *Internal Audit* view, and choose *Propose Risk*.

> i Note
>
> You need to assign the risk to an organizational unit that exists in Risk Management before proposing the risk. The system pushes the risk data to the target system via the connector that you used to import the organizational unit. You can find more information about master data import and connectors in Customizing activities *Import Master Data* and *Set Up Connectors*.

5.3 Controls

Use

The *Controls* tile allows you to access the central repository for storing controls imported from other systems or proposed by the audit team. Controls are categorized by different views. SAP Audit Management has the following default views:

- *Internal Audit* (`IA`): Controls in the IA view can be assigned to audits for control assessment and testing.
- *Risk Management* (`RM`): The RM view is used to store imported controls from SAP GRC systems.

You can add new views via Customizing activity *Maintain Views for Risks and Controls*.

You can switch from one view to another to display the controls under the view. You can import controls between views, provided that you have the corresponding authorization to access the view. For more information, see the documentation for authorization object `AUD_VIEW`.

You can find the following information when you display a control:

Field	Description
ID	The ID is automatically generated by the system. You can define the number range for the ID in Customizing activity *Maintain Number Ranges for Risks and Controls*.

Field	Description
Status	Possible control statuses are *Draft* and *Active*
Title	Title of the control
Organization	Organization assignment
Description	Description of the control
Validity	Validity of the control
Control Category	Control category, control significance, control automation, and nature of control are four basic attributes of a control. The values of control category, control significance, and nature of control are defined in Customizing activity *Maintain Control Attribute Values*. Control automation values are brought over from the source system during import.
Control Significance	
Control Automation	
Nature of Control	
Source System	Name of the source system from which the control is imported
Source Object	The ID of the control object in the source system, displayed as a hyperlink

The *Risks* tab shows all the risks that the control has been assigned to as a response.

The *Findings* tab shows all the findings that have been created during auditing.

The *Tests* tab shows all tests that have been performed on the control. Test history can also be imported from a source system.

Creating controls

During an audit, you might find inadequate or ineffective controls in an organization. To support the organization in the management of risks and control processes, the audit team can propose new controls to the auditee. You can create controls in the *Internal Audit* view only. To create a new control:

1. Go to the *Controls* screen and select the *Internal Audit* view.
2. Choose *Create* and enter the following information:
    - Title: Title of the control.
    - Organization: Choose an organizational unit to assign the control to.
    - Description: Description of the control.
    - Validity: Enter the valid dates of the control.
    - Control Category, Control Significance, Control Automation, and Nature of Control: Choose values for the control attribute fields.
    - Status: Choose a status for the control. Possible statuses are *Draft* and *Active*.
    - Risks: Select and add risks that the control is designed to cover.
3. When you finish, save the control.

Mass Upload of Controls

You can upload sets of controls using spreadsheet to mass define controls that you have already created elsewhere.

On the *Controls* screen, click *Download Template*. When the download is complete, open the template and enter the required information. Save and upload the completed spreadsheet.

For more information about using the template, see Working with Spreadsheet Templates [page 32].

Assigning controls to risks as responses

The *Risks* tab of a control displays a list of risks that the control has been assigned to as response. You can also find a list of controls on the *Controls* tab of a risk. This risk-control matrix, that is, the relationship between risks and controls, can be either created manually or imported from SAP Process Control and SAP Risk Management. To create risk-control relationship manually, go to the *Risks* tab of a control and assign it to a risk by choosing the + (*Add*) button.

Controls are time-dependent

Controls are time-dependent. That means the control information you see on the *Controls* screen is the information the control had at the time of the last import. Each time a control is imported from the GRC system or from another view, it is updated with the latest information. A control may have different information under different views.

More Information

Risk Register [page 24]

5.4 Dimensions

In SAP Audit Management, you can use dimensions to categorize or characterize auditable items. Dimensions also let you assign risk scores to auditable items.

Dimensions are organized into categories, such as Organization, Country, Line of Business, that you can freely define in Customizing. Defining a dimension lets you establish a characteristic within one of these categories, perhaps individual countries. You can then set the risk score for your dimension and use it to characterize auditable items. You can change the risk score over time.

> Example
>
> Assume that an external audit is coming up for a particular lab in your organization. You could use dimensions to connect auditable items that pertain to the lab and to express the relative urgency of these items in view of the upcoming audit. You might then define a type of dimension called `Labs`. Within this dimension type, you could then define a dimension for the lab in question. You could assign an urgency to these auditable items by setting a risk score for the dimension. You could even increase the risk score over time to ensure that the auditable items are processed before the external audit takes place.

Defining Dimension Types

Define categories of dimensions and initialize the number range for dimensions in the Customizing of SAP Audit Management. You can open the Customizing tree in the SAPGUI front end client with transaction `GRCAUD_IMG`. The path to the activities is as follows: ▶ *SAP Audit Management* ▶ *Master Data* ▶ *Dimensions* ◀.

Defining Dimensions and Setting Risk Scores

To define a dimension and set a risk score, do the following:

1. Open the *Dimensions* tile on the *Home* screen.
2. Choose the dimension type for your dimension and click *Create*.
   (If you just want to change the risk score, then just click an existing dimension in the list.)
3. Enter a *Title* and *Description* and save the dimension.
   You can further create children for the dimension. To do so, go to the *Children* tab of the dimension and choose *Add*. You can create as many levels of dimension nodes as you want.
4. To assign or change a risk score, click the dimension in the list of dimensions.
5. On the dimension details screen, click the **+** icon. In the *Add New Key Risk Indicator* dialog, set the current risk score. The score remains in effect for the dimension until you or another user sets a new risk score. The *KRIs* (Key Risk Indicators) button lets you display the risk scores of a dimension.
6. On the *Risks* tab, you can add any number of risks from the *Internal Audit* view. Risks can be assigned to a dimension to help determine its risk score.

You can now assign your dimensions to auditable items and audits. An auditable item or audit can have as many dimensions as you wish to assign to them. For more information, see Create Auditable Items [page 35] and Edit, Delete and Initiate audits [page 53].

Mass Definition of Dimensions

You can upload sets of dimensions within a category to mass-define dimensions or to take over dimensions that you have already defined elsewhere.

From the start screen of *Dimensions*, click *Download Template*. When the download of the spreadsheet has completed, enter the *Titles* and *Descriptions* of your dimensions. You can also upload an existing spreadsheet that offers the same columns as the download template. Use the *Upload* button to upload your completed spreadsheet.

For more information about using the template, see Working with Spreadsheet Templates [page 32].

5.5 Importing Master Data

Use

Master data can be imported from SAP GRC systems, for example, SAP Process Control and SAP Risk Management. Risks and controls can also be imported from one view to another.

Importing Master Data from SAP GRC Systems

The following information can be imported from SAP GRC systems:

- Risks
- Controls
- Risk analysis results
- Risk-control matrix
- Control test steps
- Control test history
- Organizational units
- Assignment of organizational units to risk and controls

> i Note
>
> The assignment relationships are created at the import of risks and controls. Organizational units must be imported prior to the import of risks and controls.

To keep your master data up-to-date, you can schedule background jobs for regular import.

For more information about importing master data from GRC, see the Customizing activity *Importing Master Data*.

Importing Risks and Controls Between Views

You can also import risks and controls from one view to another. To do so:

1. Go to *Risk Register* or *Controls*.
2. Switch to the view you want to import the object to and choose *Import*.
3. On the import screen, switch to the view you want to import the object from, select the items, and choose *OK*.

> i Note
>
> When you import risks and controls, copies of the objects are created under the specified view. If risk-control assignment relationships exist in the source system or source view, the relationship are also replicated when both the concerned risk and control are imported.

More Information

Risk Register [page 24]

Controls [page 27]

Organizations [page 22]

5.6 Working with Spreadsheet Templates

SAP Audit Management provides the functionality for users to upload data using standard templates. For example, you can download a template, maintain data offline for controls, risks, dimensions, auditable items, and work programs, and upload it to the system. These standard templates are delivered by SAP and are designed to work with most spreadsheet tools. However, there are a few tips that you need to know before you jump in and maintain the data.

- **Required and Optional Fields**
  Required fields are distinguished from optional fields by an asterisk (*). You must make an entry in all required fields to successfully upload data.

  > i Note
  >
  > In the work program template, required fields are not marked.

- **Valid Input Area**
  Each template has a valid input area. Only the data within the valid input area are recognized and uploaded to the system. By default, the first row after the heading row is marked as the valid input area. You can expand this area by placing your cursor over the lower-right corner of the area and dragging it to the desired position.
- **Data Validation**
  Data validations may be applied to the cells where restriction of data input is needed. Here is a list of input formats you'll see in a template:
  - Drop-down list: select values from the list only.
  - Date: enter a date in the correct format. To check which date format is accepted, press `CTRL` + `;`, and the current date will be displayed. Enter your date in the same format.
  - User: only NetWeaver user names are accepted.
  - Text: length limit may be applied to a text field.
- **Text Format**
  Make sure you enter texts without any formatting in the cells. Formatted texts may cause unexpected errors during upload and are not recognized by the system.

6 Planning

Audit planning is the initial phase of the auditing process. During this phase, the overall auditing strategies and focus areas for your organization are defined, the audit plan for the upcoming audit period is prepared, and audit resources are arranged for the planned audits. Auditable items, audits, and audit plans are created in this phase.

The following topics are covered in this phase:

- Audit Universe [page 33]
- Audits [page 47]
- Audit Plans [page 39]
- Managing Audit Resources [page 57]
- Recording Time [page 59]

6.1 Audit Universe

The audit universe is a collection of all auditable items in an organization.

The audit universe displays a list of auditable items with basic information such as ID, title, status, creation date and so on. You sort and filter the auditable item list by clicking the *View Settings* button. You can also personalize the columns in *Personalization*.

From the audit universe, you can:

- Create, edit, and release auditable items
- Assign risks and dimensions
- Upload attachments
- View other auditable item details, including the assigned audit history, life cycle status, and administrative information

To perform the above actions, you must have the relevant authorizations for your user.

To access the audit universe, simply click the *Audit Universe* tile on your *Home* screen.

> i Note
>
> You can only access the audit universe with the right authorization. For more information, see Roles in SAP Audit Management [page 12].

Displaying Additional Information

You can use the *Personalization* button to include additional columns in the auditable item list, such as the latest audit information and organization information. The following additional columns are available:

- Information on the last audit created for the auditable item:
    - Latest Audit ID

    - Latest Audit Title
    - Latest Audit Status
    - Actual Time Period of Latest Audit

> i Note
>
> The latest audit information is determined by the actual start date of the audit.

- Organization Information
    - Organization ID
    - Organization Title
    - Organization Group
- Auditable item release status
    - Life Cycle Status

You can use the above fields to personalize the auditable item list. You can also use them to sort, filter, and group the auditable items.

More Information

Auditable Items [page 34]

6.1.1 Auditable Items

An auditable item is a process, activity, program, or risk that can be audited. Auditable items are created in *Audit Universe* or *Create Auditable Item* upon request.

An auditable item is open or closed. A closed auditable item can no longer be used until you reopen it.

An open auditable item can have different status.

In *Audit Universe*, an open auditable item is marked with one of the following statuses.

Status	Description
New Master	This auditable item has never been released. Only released auditable items can be assigned to audits or audit plans.
Released Master	This auditable item has been released and no updates exist.
Released & Updated Master	This auditable item has an update since its last release but the update has yet to be released.

If an open auditable item is released and assigned to an audit or an audit plan, you can check it in that audit or audit plan, where the auditable item is marked with one of the following statuses.

Status	Description
Active	This auditable item is the latest released version.
Outdated	This auditable item has a released update. You may need to refresh to get its latest version.

Open an auditable item in *Audit Universe* and you can find the following information.

Section	What information you can find here?
Header	Auditable item ID, group, requesting person and date, responsible person, and the auditable item status
General Information	General information about the auditable item, including: risk level, impact level, likelihood level, estimated effort for business, estimated effort for IT, risk score, highest risk score, source, description, and tags.
Audit History	A list of audits that the auditable has been assigned to. You can navigate to the audit screen from the links.
Risks	A list of risks assigned to the auditable item
Dimensions	A list of dimensions the auditable item is associated with
Attachments	A list of attachments uploaded to the auditable item
Administration Data	The version, create date, last changed date, and the last release date (if applicable) of the auditable item

More Information

Creating and Editing Auditable Items [page 35]

Deleting Auditable Items [page 38]

6.1.1.1 Create Auditable Items

Use

You can create an auditable item in the app *Create Auditable Item* or *Audit Universe*.

When creating or editing an auditable item, you are asked to provide the following information:

Field	Required/Optional	Description
Title	Required	A descriptive name for an auditable item, to help users identify the item.
Organization	Optional	You can select an organizational unit to assign the auditable item to.
Requested by	Required	The name of the person who requested that an auditable item be added to the audit universe.
Group	Required	The authorization group to which an auditable item is assigned. A user must have an authorization for the group and the desired action in order to work on an auditable item. The available authorization groups are defined in the Customizing under *Define Audit Groups*. The authorization object that is used is `AUD_ITEM`.
Requested on	Optional	Date of request
Risk Level	Optional	An estimate of the overall risk that irregularities in an auditable item pose to an enterprise or other organization. The risk level reflects both the impact of irregularities and the likelihood that irregularities exist in an auditable item. SAP delivers a default set of risk levels. You can modify these levels in the Customizing under *Maintain Risk Levels*.
Impact Level	Optional	An estimate of the effect on an enterprise or other organization if irregularities occur in an auditable item. SAP delivers a default set of impact levels. You can modify these levels in Customizing under *Maintain Impact Levels*.
Likelihood Level	Optional	An estimate of the likelihood that irregularities are present in an auditable item. SAP delivers a default set of impact levels. You can modify these levels in Customizing under *Maintain Likelihood Levels*.
Estimated Effort for Business	Optional	An estimation of required person days for business personnels to execute the audit

Field	Required/Optional	Description
Estimated Effort for IT	Optional	An estimation of required person days for IT personnels to execute the audit
Risk Score	Optional	An estimation of risk score for the auditable item. The risk score value ranges from 0 to 100.
Source	Optional	Information on the background or motivation for requesting an auditable item.
Description	Optional	Detailed information on an auditable item, as required to help identify the scope of the item, the activities involved, and so on.
Responsible Person	Optional	The person responsible for an auditable item. This may be a person in the audit organization or it may be the contact person in the organization to be audited; you may use this field as you wish.
Tags	Optional	Search tags that you assign to an auditable item to classify it and make it easier to find. The system suggests already existing tags based on the characters that you have typed in. But you can add your own new tags as well, simply by typing them in.

After an auditable item is successfully created, the system automatically assigns a numeric ID to it. You can define how the system generates this ID in Customizing activity *Maintain Number Range for Auditable Items*.

Assigning risks to auditable items

You can assign risks from *Risk Register* to auditable items for risk-based auditing. To do so, navigate to the *Risks* tab of an auditable item, choose + (*Add*), select the risks on the *Add Risks* screen, and choose *OK*.

For more information about risks, see Risk Register [page 24].

Assigning dimensions to auditable items

You can assign dimensions to auditable items to help determine its risk score. When you assign multiple dimensions to an auditable item, the largest risk score appears in the *Highest Risk Score* field of the *General Information* tab. To assign a dimension, navigate to the *Dimensions* tab of the auditable item, choose + (*Add*), select the dimensions, and choose *OK*.

For more information about dimensions, see Dimensions [page 29].

> i Note
>
> The highest risk score from assigned dimensions can be used to help decide the overall risk score of the auditable item. For example, you create a new auditable item and assign three dimensions to it. In the *Highest Risk Score* field, the largest risk score of the dimensions is displayed as a suggestion for you to determine the overall risk score for the auditable item.

Adding attachments to auditable items

After you create an auditable item, you can upload attachments to it. To do so, navigate to the *Attachments* tab of the auditable item, choose + (*Add*), select the file to upload, and choose *OK*.

Releasing auditable items

On the *Administration Data* tab, you can find the date and time of last release in the *Release Timestamp* field. The field is not displayed if the auditable item has never been released.

Mass Upload of Risks

You can upload sets of auditable items using spreadsheet to mass define the items that you have already created elsewhere.

In *Audit Universe*, click *Download Template*. When the download is complete, open the template and enter the required information. Save and upload the completed spreadsheet.

For more information about using the template, see Working with Spreadsheet Templates [page 32].

More Information

- Auditable Items [page 34]
- Deleting Auditable Items [page 38]

6.1.1.2 Close and Delete Auditable Items

Close auditable item

You can exclude an auditable item from use in audits by closing it. To do this, find it in *Audit Universe*, click *Edit* and change its status to *Closed*, then release it.

Closed auditable items remain in the system. You can reopen a closed auditable item, if it is needed for audits again.

Delete auditable item

If you want to delete one or more auditable item permanently from the system, then do the following:

1. Log on to the back-end System of SAP Audit Management. Log on to a client other than the production client.
   You can display the role of a client – production or some other role – by choosing *SAP Menu* > *Tools* > *Administration* > *Administration* > *Client Administration* > *Client Maintenance*. The *Client role* field in *Details* shows whether a client is a production client.
2. Choose *SAP Audit Management* > *Tools* > *Delete Auditable Items*, or enter transaction `GRCAUD_DEL_AUD_ITEM` (*Report for deletion of Auditable Items*) in the command field.

3. Use the selection screen to identify the auditable item or items that you want to delete.
4. Select *Execute* to run the transaction.
   The transaction reports how many auditable items have been selected for deletion and asks you to confirm the deletion.
5. If you confirm the deletion, then the transaction removes the auditable items from the database. When it is done, it displays a confirmation message reporting how many of the selected auditable items were deleted. Any auditable items that could not be deleted remain unchanged in the database.

6.2 Audit Plans

An audit plan is a plan created by an audit manager or a CAE based on the organization's risk assessment and the input of senior management, on which auditing personnel follow through to achieve auditing goals. An audit plan includes auditing tasks that need to be completed within a period of time.

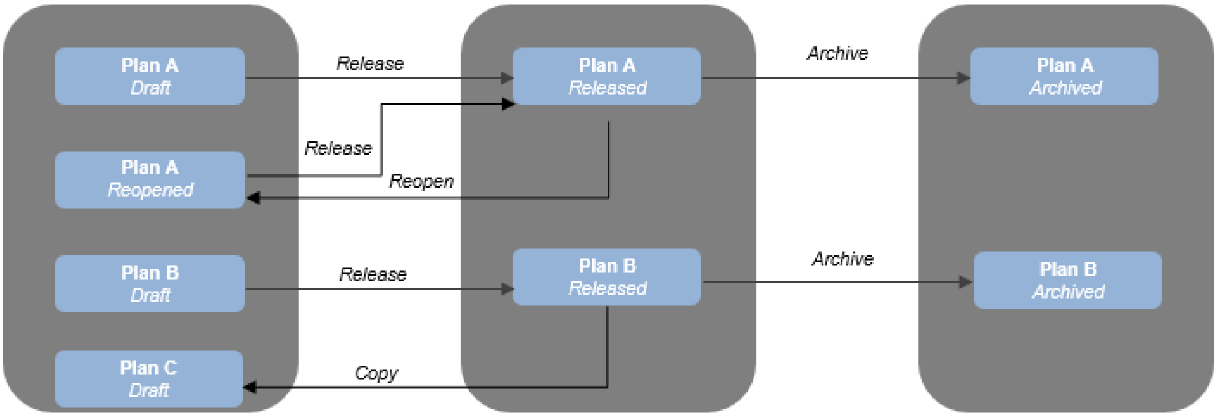
Audit Plan Status

An audit plan has one of the following statuses:

- Draft: A newly created audit plan is automatically marked as draft. You can plan your auditing tasks in a draft audit plan.
- Released: When you have finished your planning in a draft audit plan, you can release it, then your audit team will start auditing work according to the released plan. A released audit plan cannot be modified unless you reopen it.
- Reopened: If you want to make changes to a released audit plan, you have to reopen it. A reopened audit plan can be edited and released again.
- Archived: When all the auditing tasks involved in a released audit plan have been completed, the audit plan has reached the end of its life cycle. You can archive it.

You can have multiple draft, reopened, and released audit plans at the same time so you can plan auditing for different organizations, processes, and areas.

The figure below shows how an audit plan can change between statuses:



Audit Plan Status

Audit Plan General Information

The *General Information* of an audit plan includes:

Field	Required/Optional	Description
Title	Required	A descriptive name for an audit plan to help users identify the plan.
Time Period	Required	The planned running time of the plan, expressed as starting and ending dates. These dates help determine which audits may be selected for a plan; see the previous section for more information.
Planned Effort	Optional	Use this field to aggregate the effort involved for audits in the audit plan. You can also express any synergistic effects that might reduce the effort. The field is denominated in person workdays.
Estimated Effort for Business	Optional	An estimation of required person days for business personnel to execute the audit. The value of this field is aggregated from the fields of the auditable items assigned to the audit plan. You cannot edit the field manually.
Estimated Effort for IT	Optional	An estimation of required person days for IT personnel to execute the audit. The value of this field is aggregated from the fields of the auditable items assigned to the audit plan. You cannot edit the field manually.

Field	Required/Optional	Description
Financial Budget	Optional	Use this field to aggregate the budgets planned for audits in the audit plan. You can also express any synergistic effects that might reduce the total cost of the plan. The field is denominated in the application currency, shown to the right of the field.
Total Estimated Effort from Audits	Optional	The total effort and cost are automatically calculated from all audits included in the audit plan.
Total Actual Effort from Audits		
Total Estimated Cost from Audits		
Total Actual Cost from Audits		
Description	Optional	Use this field to enter detailed information on an audit plan to help identify the scope of the plan; such as the year or quarter it takes place in, whether it is a special project, as well as any other high-priority information on the plan.

6.2.1 Creating Audit Plans

To create a new draft audit plan, in the *Manage Audit Plans* app, choose the *+ (Add)* button on the initial page and fill in all required fields.

The initial page provides access to all the existing audit plans. You can view plans by status, or use the search function to find specific plans. Select an audit plan, and you will navigate to its main page where you can check or maintain the content of the plan.

6.2.2 Maintaining Audit Plans

Draft and reopened audit plans can be modified. You can edit their general information and add or remove risks, auditable items or audits.

Editing Audit Plans

Choose a draft or reopened audit plan and navigate to its main page.

To Add Risks

In *Risks* section you can add, remove and search for risks. To add risks, choose the *+* button, and a window that shows a list of risks will open. Only the risks contained in the *Internal Audit* view of the *Risk Register* are displayed in this list.

If a risk that has been added to the plan is also covered by an auditable item, the auditable item can be directly added to the plan by selecting the risk and using the *Add Auditable Items* button in the *Risks* section.

To Add Auditable Items

In the *Auditable Items* section, you can add or remove auditable items. If an auditable item covered by your plan is updated in the *Audit Universe*, you can remove the old version from your plan and add the latest version.

To Add Audits

In the *Audits* section, you can add existing audits to your audit plan or remove unwanted audits. An audit can be included in an audit plan if the following conditions are met:

- The audit is open. You cannot add audits with Closed or Canceled status.
- The time period of the audit overlaps with that of the audit plan.

You can also create a new audit in the *Auditable Items* section. To do this, select one or more auditable items in the *Auditable Items* section and choose the *Create Audit* button. The new audit that this creates covers the selected auditable items and is automatically included in the plan.

> i Note
>
> A risk is automatically added to an audit plan when you add an auditable item that covers the risk to the plan. To enable this functionality, from the SAP GUI, enter transaction `SM34`, enter view `GRCAUD_V_ATRKFAD`, and choose *Maintain*. On the view maintenance screen, activate the Customizing item `AUD_AUTO_RISK_FADTBL`.

Deleting Audit Plans

You can delete a draft audit plan if you don’t need it. To do so, select a draft audit plan, and choose the *Delete* button at the top-right corner of its main page. Note that the deletion of a plan does not erase the risks, auditable items or audits that have been added to the plan.

6.2.3 Releasing Audit Plans

After you have completed the planning work in a draft audit plan, you can release the plan by choosing the *Release* button located at the top-right corner of its main page.

Released audit plans are not modifiable. If you want to make changes to a released plan, for example, to include additional audits, you need to reopen it.

6.2.4 Reopening, Copying and Archiving Audit Plans

Reopening Audit Plans

To enable editing of a released audit plan, you have to reopen it first by choosing the *Reopen* button on its main page. Reopened plans can be edited and released again.

Copying Audit Plans

A new draft audit plan can also be created by copying from a released plan. The general information and the risks, auditable items, and unfinished audits included in the released plan will be copied to the new draft plan. The new plan shares the name with the released plan, but has a different ID.

When to copy a released audit plan?

If the auditing tasks covered by a released audit plan haven't been finished within the planned time period, you can carry the unfinished audits on to a new plan for the upcoming auditing period. You can do this by copying the released plan to a new draft plan. As a result, the unfinished audits are automatically copied to the new draft audit plan.

Archiving Audit Plans

When all the audit tasks included in a released audit plan have been completed, the plan has reached the end of its life cycle. You can archive this plan. An archived audit plan can no longer be reopened or worked on. An audit plan can be archived in two ways:

- If a released audit plan has never been copied, you can archive it manually by choosing the *Archive* button.
- If a released audit plan has been copied to a new draft plan, it is automatically archived when the draft plan is released.

6.2.5 Risk Coverage in an Audit Plan

Use

The introduction of risks in SAP Audit Management allows the internal audit department to plan their auditing activities based on the risks of the organization. When creating and maintaining an audit plan, you can see the risks that are relevant for internal auditing and how they are covered by auditable items and audits. With the risk coverage data, the CAE and the audit manager can create audit plans and direct the audit activities with a clear focus.

A risk can be covered by both auditable items and audits in an audit plan. On the *Risks* tab of the audit plan, the numbers in the *Auditable Items* and *Audits* columns indicate how many auditable items and audits have covered this risk in the current audit plan. You can click on the numbers to display the list.

How do I cover a risk with an auditable item?

To cover a risk with an auditable item, proceed as follows:

1. In the audit universe, assign the risk to an auditable item.
2. Go to the *Auditable Items* tab of the new or draft audit plan and add the auditable item to the plan.
3. Save the audit plan. You can see the number in the *Auditable Items* column changes for the risk after you refresh the audit plan.

How do I cover a risk with an audit?

To cover a risk with an audit in an audit plan, proceed as follows:

1. In the audit universe, assign the risk to an auditable item.
2. Create an audit with the auditable item, or assign the auditable item to an existing draft audit.
3. As the audit manager, go to the *Risks* tab of the audit and add the risk under the auditable item to the audit.
4. Go to the *Audits* tab of the audit plan and add the audit to the plan.
5. Save the audit plan. The number in the *Audits* column changes for the risk after you refresh the audit plan.

More Information

Audit Plan [page 39]

6.2.6 Legacy Audit Plan Apps

You can alternatively use our legacy apps *Create Audit Plan*, *Maintain Audit Plans*, *Display Released Audit Plans*, *Display Archived Audit Plans* to do your audit planning work.

6.2.6.1 Creating Audit Plans

Creating New Audit Plans

Use the *Create Audit Plan* app to create a new plan. Newly created audit plans are added to the list of *Maintain Audit Plans* with status *Draft*.

Copying from Released Audit Plans

You can also create a new audit plan by copying from a released plan. When you copy a released audit plan, its general information, risks, auditable items, and audits are copied to the new plan. You can find the plan in *Maintain Audit Plans* with status *Draft*.

Deleting Audit Plans

You can delete a draft audit plan when you no longer need it. Note that the deletion of a plan does not erase any of the items included in the plan.

Related Information

Maintaining Audit Plans [page 45]

6.2.6.2 Maintaining Audit Plans

On the screen displayed by *Maintain Audit Plans*, you can maintain draft and reopened plans which your organization currently is working on. You can change the information, add or remove risks, auditable items, and audits from the plans. You can also find a list of risks from the *Internal Audit* view and check the coverage information of each risk.

When an audit plan has reached the desired level of completion, you can also release it. The system does not check the status of audits in the plan; you must verify that these audits have the intended status.

To Add Risks

On the *Risks* tab, you can add any number of risks from the *Internal Audit* view to the audit plan by choosing the + (*Add*) button. This allows you to create a risk-based audit plan. You can then check the coverage of the risks and plan the audit activities accordingly.

If a risk has been assigned to an auditable item, you can also add it to plan by selecting the risk and choosing *Add Auditable Items*.

To Add Auditable Items

You can add auditable items to an audit plan by choosing the + (*Add*) button. The system displays a list of the *Active* auditable items at the current time and you can select the items you want to add to the plan. If the auditable item is updated and released later on in the audit universe, the version you added to the audit plan becomes outdated. If you want the latest version in the plan, you can remove and reassign the auditable item.

> i Note
>
> Risks can be automatically added to an audit plan when you add the related auditable items. To enable this functionality, go to transaction `SM34`, enter view `GRCAUD_V_ATRKFAD`, and choose *Maintain*. On the view maintenance screen, activate the Customizing item `AUD_AUTO_RISK_FADTBL` to allow the system to automatically assign risks.

To Add Audits

A single audit may belong to more than one audit plans. For example, you may start an audit under one plan and carry it forward to the next plan.

To include an audit in an audit plan, go to the *Audits* tab, choose + (*Add*), select the audits you wish to add to the plan, and choose *OK*. You may select audits that fit these criteria:

- The audit is active. You cannot add audits in status *Closed* or *Canceled*.
- The time period of the audit overlaps with that of the audit plan. That is, the audit start date must be earlier than the end date of the plan, and the audit end date must come after the start date of the audit plan.

You can also go to the *Auditable Items* tab and create an audit directly from the plan. Audits created within an audit plan are automatically included in the plan.

6.2.6.3 Releasing Audit Plans

After you complete the planning, you can release a draft audit plan by clicking the *Release* button. The release of an audit plan freezes all information under the plan, including risks, auditable items, and audits. You are not able to add, create, or remove any of these objects or edit the general information unless you reopen the plan.

Released audit plans can be reopened or archived.

Related Information

Reopening Audit Plans [page 46]

6.2.6.4 Reopening Audit Plans

Released audit plans can be reopened and reworked with so that you can include additional audit activities in the plan.

You can reopen an audit plan in *Display Released Audit Plans*. Reopened plans are added to the list of *Maintain Audit Plans* with status *Reopened*.

Related Information

Maintaining Audit Plans [page 45]

6.2.6.5 Archiving Audit Plans

When all audit activities planned have been completed and the audit plan has reached the end of its lifecycle, you can move it to the archived audit plan list. An archived audit plan can no longer be reopened or worked on.

You have two options to archive an audit plan:

- If a released audit plan has never been copied, you can archive it manually in *Display Released Audit Plans*.
- If a released audit plan has been copied to a new plan, it is automatically archived when you release the draft plan.

You can access archived audit plans in *Display Archived Audit Plans*.

Related Information

Releasing Audit Plans [page 46]

6.3 Audits

In SAP Audit Management, an audit is a process that defines the time, scope, resource as well as other attributes for an audit engagement, and documents evidences, results, recommendations and reports.

What information can you find in an audit?

The detailed information of an audit is displayed under different tabs. The following is a list of tabs and the information you can find on the detail screen:

Tab Name	What information is displayed?
Info	The general information of the audit, including: ID, Title, Status, Audit Scope, Executive Responsible, Time Period, Group, Category, Country, Country Code, Estimated Effort, Estimated Cost, Actual Time Period, Actual Effort, Actual Cost, and Tags. If auditable items are assigned to the audit, you can also see them listed under the Auditable Items section. You can navigate to an auditable item by clicking on the list entry. Actual Time Period, Actual Effort, and Actual Cost information is only visible when the audit is initiated.
Team	A list of team members assigned to the audit, with a badge on the icon indicating the number of users assigned to the audit.
Activity History	If activity logs are activated, an entry that describes the activity will appear in the *Activity History* tab. For more information about activating activity logs, see the customizing activity *Maintain E-mail Notifications for Audit Activities*.

Tab Name	What information is displayed?
Work Program	The work program for this audit (if any).
Working Paper	A list of working papers (if any) under the work program, with a badge on the icon indicating the total number of working papers under the audit. The default view displays the work program in a folder structure. You need to navigate to the specific work package to view the working papers assigned.
Finding	A list of findings (if any) under this audit, with a badge on the icon indicating the total number of findings.
Report	A list of reports (if any) created for this audit, with a badge on the icon indicating the total number of reports.

> **i Note**
>
> The Working Paper, Finding, and Reporting tabs are only visible after the work program is approved.

Audit status

Audit status indicates the progress of an audit in its lifecycle. The following table lists all the audit statuses in SAP Audit Management, and explains what you can do under each status.

Audit Status	What does it mean?	Who can access this audit?	What can you do under this status?
Draft	When an audit is created and saved as draft, it has the *Draft* status.	Audit manager	Edit, initiate, or delete the audit.
Initiated	When an audit is initiated, the status becomes *Initiated*.	Audit lead	Edit the audit. Prepare and submit work program.
Announcement Submitted	The announcement letter has been submitted for review.	Audit manager	Review, approve, or reject the announcement letter
Announcement Rejected	The announcement letter has been rejected by the audit manager.	Audit lead	Revise the announcement letter and submit again
Announcement Approved	The announcement letter has been approved by the audit manager..	Audit manager	Distribute announcement letter to stakeholders
Announcement Distributed	The announcement letter has been distributed.	Audit lead	Proceed to prepare work program

Audit Status	What does it mean?	Who can access this audit?	What can you do under this status?
Work Program Submitted	When a work program is submitted, the audit status becomes *Work Program Submitted*.	Audit manager	Edit the audit. Review, approve, or reject the work program.
Work Program Rejected	When the work program is rejected, the audit status becomes *Work Program Rejected*.	Audit lead	Edit the audit. Revise and submit work program.
Work Program Reopened	When an auditor reopens the work program of an audit, the audit status becomes *Work Program Reopened*.	Audit lead	Edit the audit. Revise and submit work program.
In Execution	When the work program is approved, the audit enters the *In Execution* status.	Audit lead Auditors	Edit the audit. Create working papers. Create findings Create audit reports. Submit audit reports (only for audit lead).
Draft Report Submitted	When a draft report is submitted for review, the status becomes *Draft Report Submitted*.	Audit manager	Edit the audit. Review, approve, or send the draft report back for rework.
Rework Draft Report	When the audit manager sends back the draft audit report for rework, the status becomes *Rework Draft Report*.	Audit lead	Edit the audit. Modify the draft report, and submit it again for review.
Draft Report Approved	When the draft audit report is approved, the audit status becomes *Draft Report Approved*.	Audit lead	Edit the audit. Submit a final audit report.
Final Report Submitted	When the final audit report is submitted for review, the audit status becomes *Final Report Submitted*.	Audit manager	Edit the audit. Review, approve, or send the final report back for rework.

Audit Status	What does it mean?	Who can access this audit?	What can you do under this status?
Rework Final Report	When the audit manager sends back the final report for rework, the status becomes *Rework Final Report*.	Audit lead	Edit the audit. Modify the final report, and submit it again for review.
Final Report Approved	When the final audit report is approved, the audit status becomes *Final Report Approved*.	Audit manager	Edit the audit. Distribute the audit report. Close the audit.
Final Report Issued	You can issue the audit report in *Issue Audit Reports* tile after the final report has been approved. This status is acquired after the report is distributed.	CAE Audit manager Audit Lead	N/A
Closed	You can close an audit when the final report is approved. After closing an audit, the status becomes *Closed*. Closed audits can be accessed from the *Display Historical Audits* tile.	All i Note Your user must have the corresponding group authorization to display audits under that group.	View audit information.
Canceled	Audits can be canceled after it is initiated and before the final report is approved. You can find *Canceled* audits in *Display Historical Audits*.	CAE Audit manager	N/A

Above is the predefined audit status schema delivered by SAP Audit Management. You can customize how audits change from one status to another, and which users are allowed to access audits under a specified status in customizing activity *Define Audit Status Schema*.

Where to find an audit of a specific status?

Audits can be accessed from different tiles depending on the role of your user and the audit status. For more information about where to find an audit of a specific status, see Available Apps [page 19].

Exporting Audits

The export function on an audit list screen allows you to export and download the complete list of audits available to your user. This allows you to view and track audit status offline, for example, using a spreadsheet tool.

To enable this function, you need to first maintain the file templates in scenario `LST_AUDIT` in customizing activity *Maintain Templates for File Generation*. This scenario is offered in the default setting.

To export the audit list, click the *Export* icon on top of the audit list and choose the desired export format.

> **i Note**
>
> The exported document contains the complete list of audits and all information available to the audits, regardless of the personalization and filters applied to the list.

More Information

Create Audits [page 51]

6.3.1 Create Audits

You have the following ways to create a new audit:

- On the *Home* screen, choose the *Create Audit* tile to create a new audit.
- In the *Manage Audit Plans* tile, go to the *Auditable Items* tab of a draft audit plan, select one or more auditable items from the list, and choose *Create Audit*.
- On the initial screen of the *Initiate Audits* Fiori app, click + (*Create Audit*)

On the *Create Audit*/*New Audit* screen, you will be asked to enter the following information:

Field	Required/Optional	Description
Title	Required	A descriptive name for the audit; the maximum length is 100 characters.
Audit Scope	Required	A short, general description of the overall scope of the audit, for example, the activity or process to be audited, and what the audit intends to achieve.
Time Period	Required	Choose the start date and end date of the audit.
Type	Required	Select the audit type from the dropdown list. Audit types are defined in Customizing activity *Define Audit Types*.

Field	Required/Optional	Description
Group	Required	The authorization group to which the new audit is assigned to. A user must have the authorization for the group in order to work on an audit. The available authorization groups are defined in Customizing activity *Define Audit Groups*.
Category	Required	Select a category from the drop-down list for the new audit. The available audit categories are defined in Customizing activity *Define Audit Categories*.
Country/Region	Optional	The country or region of the organization to be audited. The available countries and regions are defined in Customizing activity *Specify Countries in SAP Audit Management*.
Company Code	Optional	Enter the company code of the organization to be audited.
Estimated Effort	Optional	Estimate the effort (in person days) to be spent on the audit.
Estimated Cost	Optional	Estimate the cost to be spent on the audit. The cost currency can be maintained in Customizing activity *Maintain Audit Currency*.
Tags	Optional	You can add tags for an audit, so that it can be easily searched using the search function. You can add multiple tags for one audit. The maximum length for a single tag is 20 characters.

You can also add or remove the auditable items assigned to the new audit.

When you finish, choose *Save* to save the audit. The audit is then saved with the status Draft and can be accessed from the *Initiate Audits* tile. You can maintain team member information, edit, delete or initiate the audit.

Uploading audits using spreadsheets

Alternatively, you can use a spreadsheet template to mass upload audits to the system:

Go to the *Initiate Audits* tile, download the template, maintain audits offline in the template, and upload it to the system.

For more information about using the template, see Working with Spreadsheet Templates [page 32].

More Information

Audits [page 47]

Edit, Delete and Initiate audits [page 53]

6.3.2 Edit, Delete and Initiate audits

Draft audits can be found in the *Initiate Audits* app.

In the app, select a draft audit and go to its detail page, you can then edit its general information, assign people to roles such as audit manager and add auditable items, risks,organizations and dimensions to it. After these work has been done, the audit manager can initiate the draft audit to bring it into the preparation phase.

You can delete a draft audit if it is not needed.

Roles

You can appoint **Audit Manager**, **Audit Lead**, **Chief Audit Executive** and other roles for an audit. People assigned to these roles can be changed even after the audit has been initiated. **Audit Manager**, **Audit Lead** and **Chief Audit Executive**are required roles without which an audit cannot be initiated.

Add and update auditable items

In the *Auditable Items* section, you can assign auditable items to the audit. A ↻*Refresh*button will appear on an auditable item entry when this auditable item is updated and released again in *Audit Universe*, prompting you to update it to its latest released version.

For more information about auditable item release status, see Auditable Items [page 34].

Add risks

Assignment of risks to a draft audit is performed by the following ways.

- You can directly assign a risk to the draft audit in the *Risks* section .
- Following you assign an auditable item to the audit, the risks assigned to the auditable item will be automatically assigned to the audit.

  To disable this auto assignment function, go to the Customizing activity *SAP Audit Management* > *Audit Planning* > *Define Audit Types* and follow the instructions.

> i Note
>
> Only risks that can be found in the *Internal Audit* view in the app *Risk Register* are allowed to be assigned.

Add dimensions

Scroll down to the *Dimensions* section on the detail page of a draft audit, and you can assign dimensions to the audit here. Depending on your back-end configuration, you can choose dimensions from all the existing dimensions or from only those assigned to the auditable items that have been assigned to the audit.

> i Note
>
> To be able to select from all the existing dimensions, you need to enable it in the Customizing activity *SAP Audit Management* > *Audit Planning* > *Audit* > *Define Audit Types* .

Add organizations

In the *Organizations* section, you can assign organizations to the draft audit. You can choose from all the existing organizations or from only those assigned to the auditable items that have been assigned to the audit as the case it may be.

> i Note
>
> To be able to select from all the existing organizations, you need to enable it in the Customizing activity *SAP Audit Management* > *Audit Planning* > *Audit* > *Define Audit Types* .

Initiate an audit

Only the person appointed as the **Audit Manager** for this audit is able to initiate it. After an audit has been initiated, it is moved to the *Prepare Audits* app, where the audit lead of this audit can prepare the audit announcement letters and work program.

Delete an audit

You can only delete an audit when it is in the status Draft. To do this, click the *Delete* button.

More Information

Create Audits [page 51]

Prepare Audits [page 62]

6.3.3 My Ongoing Audits

Ongoing audits are audits which the audit lead and auditors actively work on. Ongoing audits range from status *Initiated* to status *Final Report Approved*. The *My Ongoing Audits* screen is the central place where the audit lead and auditors access the ongoing audits assigned to them and perform audit tasks. These tasks include processing working papers, performing audit procedures, creating findings and actions, and preparing audit reports. You can also edit the general information of the audit or change team member assignments.

> i Note
>
> To prepare audit announcement letters and work programs as an audit lead, you need to go to the *Prepare Audits* tile.

More Information

Audits [page 47]

Prepare Audits [page 62]

6.3.4 Track Ongoing Audits

The *Track Ongoing Audits* tile is available for the audit manager to track the current status of audits. The *Track Ongoing Audits* screen lists the audits assigned to you as the audit manager. You can monitor the overall progress of each audit, check the tasks performed, view the working papers, findings and reports that have been created, and close the audit.

To perform other tasks as the audit manager, go to the *Approve Audit Preparation* or *Approve Audit Report* tiles.

More Information

Review Audit Preparation [page 72]

Review Audit Reports [page 90]

Close Audits [page 91]

6.3.5 Cancel Audits

Audit manager can cancel an audit when it no longer needs to be performed. It is then moved to the *Display Historical Audits* app. A canceled audit is marked in status *Canceled* and read-only.

An audit can be canceled on one of the following conditions:

- It has been initiated and the final audit report has not been approved.
- It is in draft status and is included in an audit plan.

> ℹ Note
>
> To discontinue a draft audit which is not included in any released audit plan, you can simply delete it in *Initiate Audits*.

To cancel an audit, find it in *Track Ongoing Audits* and choose *Cancel*.

More Information

Audits [page 47]

6.3.6 Historical Audits

Use

Historical audits include canceled audits and audits that are closed after the final report is approved. Historical audits are read-only and can be accessed from the *Display Historical Audits* tile. You can view the audits only under the audit group that your user is authorized to access.

Reopening Audits

Closed audits can be reopened to allow auditors to rework the audit, for example, to add new findings and action plans.

You can reopen an audit in the *Display Historical Audits* tile. Once reopened, the audit are changed into the *In Execution* status and can be found in the *Track Ongoing Audits* and *My Ongoing Audits* tiles. As an auditor, you can add new working papers, create new findings and action plans, and submit new audit reports for review.

You can further reopen the work program of the reopened audit. For more information, see Reopen Work Program [page 74].

More Information

Audits [page 47]

6.4 Managing Audit Resources

As a CAE or audit manager, you can use the *Resource Management* app to manage audit resources, for example, to create audit teams, assign users to a team, and check the skills and calendar of each team member.

> i Note
>
> To be able to display and assign users, you need to first sync the user list with their identity providers. For more information, go to Customizing activity *Sync Audit Staff with Users from Identity Provider*.

Creating and maintaining audit teams

To create your audit teams and maintain team members:

1. Go to *Resource Management* and choose *Maintain My Team*.
2. Choose *Add* to create a new audit team.
3. In the *Add Team* dialog, enter the team name and choose *Save*.
4. Select the team to go to the detail page. Click + (*Add*) to search and add members to the team. Click *Edit* to delete members in the team.

On the *Resource Management* screen, you can select a team and check the calendar of each team member in a graphic chart. You can switch between views to display the availability by day, week, month, quarter, and year. Click on a user and go to the user profile page for detailed information, the audits performed by that user and skill information.

Setting Day Rates

Daily labor cost rates of audit team members can be set in the system, based on which the labor cost of an audit is calculated and automatically added to the actual cost of the audit, allowing the audit manager and CAE to track the auditing cost. See Setting Day Rates [page 59] for details.

More Information

To view your profile and maintain your skills as an auditor, see My Profile [page 58].

6.4.1 My Profile

Use

As an auditor, you can check your resource calendar, view all your historical and current audit engagements and other activities,, and rate your audit skills in the *My Profile* tile.

On the *Calendar* tab, you can view your audit and other activities such as leave and training marked on a monthly calendar. Click on a date to display the list of activities. Select an audit and choose *View Detail* to display the audit.

The *Audits* tab lists all audits that you have been engaged in, including historical audits, ongoing audits, and draft audits.

On the *Skills* tab, you can rate the skills for yourself.

Maintaining your skill ratings

The skill ratings help your CAE and your audit manager in planning resources for audit activities. Skills are grouped by skill sets. You can rate each skill from one to five stars. For example, you can rate your skills in business, IT, and languages.

Skills and skill sets are defined in Customizing activity *Maintain Skills for Audit Staff*.

To maintain your skills, go to *My Profile*, navigate to the *Skills* tab, choose *Edit Skills*, set the rating for the skills you want to edit, and choose *Save*.

> i Note
>
> Only you can maintain this information for yourself.

More Information

Managing Audit Resources [page 57]

Deleting Personal Data [page 59]

6.4.2 Deleting Personal Data

Use

Personal data such as skill rating and uploaded photos remains in the system even after a user leaves the audit team. With transaction `GRCAUD_DEL_PERS_DATA` or area menu *Delete Skill Data*, you can delete your personal data and the data of other users provided you have the proper authorization. You can also use this functionality to reset the skill rating of a user.

For more information about the menu, see the documentation for the transaction.

More Information

My Profile [page 58]

6.4.3 Setting Day Rates

You are able to set daily labor cost rates for audit personnel in the system, based on which the labor cost of an audit is calculated. The amount will automatically be added to the actual cost of the audit.

1. In Customizing for *SAP Audit Management*, choose *Audit Planning* > *Resource Management* > *Maintain Day Rates and Job Levels for Auditors*.
   This Customizing activity allows you to divide audit personnel into different groups and set cost rates for the groups separately. You can further define position levels within a group and set a daily cost rate for each level. For detailed instructions, see the Customizing activity documentation.
2. Open the Customizing activity *Maintain Job Levels for Auditors* (to do so, you must use the link to this activity in the Customizing activity documentation for *Maintain Day Rates and Job Levels for Auditors*).
   1. Download the Excel file that contains personnel information.
   2. In the *Staff Level ID* field of the Excel file, choose the right job level for each staff member.
   3. Return to the Customizing activity and upload the completed Excel file.
3. When the personnel working on an audit have recorded their working hours in the *Record Time* app, the system automatically calculates the costs of the personnel and adds the amounts to the actual cost of this audit, which can be checked in *Track Ongoing Audits*. In the meantime, the amounts will also be automatically added to the actual cost of the audit plan that includes this audit.

6.5 Recording Time

With the transactional app *Record Time* you can log the time you spent on audits and other activities, such as absence and training.

Key Features

You can use the calendar to pick dates and record time.

You can define non-audit activities for time recording and set maximum daily working hours in Customizing.

The system automatically calculates the total time recorded for an audit in the *Actual Effort* field.

Recorded activities appear in the calendar in Resource Management.

More Information

Recording Time for Audit Activities [page 60]

Recording Time for Other Activities [page 61]

6.5.1 Recording Time for Audit Activities

You can use the *Record Time* transactional app to log the time for audits to which you are assigned as an auditor. You can use the calendar to select dates and record the time in hours.

The system automatically calculates the time recorded for an audit as the actual effort in person days. You can find the details in the *Actual Effort* field of the audit.

> i Note
>
> The *Actual Effort* field is editable by default. To prevent its value from being changed manually during edit, we recommend that you set the field `ACTUAL_EFFORT` as read-only in the Customizing activity *Maintain Field Attributes by Status Schema*.

Procedure

1. On the calendar, select a date to record your time. You can record time for multiple dates by selecting the start date and the end date. Selected dates are highlighted.
2. In the *Details* section, choose + (*Add*) to make a new entry. The dates and duration of your selection are displayed in the entry.
3. In the *Activity Type* drop-down list, select activity type *Audit*.
4. In the *Audit* field, use the search help to choose an audit.
5. Enter the time spent on this audit in hours.

   > i Note
   >
   > You can set a limit to the maximum number of hours allowed to record per day. Do so in the Customizing activity *Limit Daily Working Hours*.
6. Choose *Apply* to save the changes.

To delete the time recorded for a specific date, select the date on the calendar, choose the *Delete* button at the end of the entry, and choose *Apply*.

More Information

Recording Time for Other Activities [page 61]

6.5.2 Recording Time for Other Activities

You can use the *Record Time* transactional app to log the time spent on non-audit activities such as absence and training. Recorded non-audit activities appear in the calendar in *Resource Management*.

Prerequisites

You have maintained non-audit activity types in Customizing activity *Maintain Activity Types*.

Procedure

1. On the calendar, select a date to record your time. You can record time for multiple dates by selecting the start date and the end date. Selected dates are highlighted.
2. In the *Details* section, choose + (*Add*) to make a new entry. The dates and duration of your selection are displayed in the entry.
3. Select the activity type and enter the number of hours spent on the activity.
4. Choose *Apply* to save the changes.

To delete the time recorded on a date, select the date on the calendar, choose the *Delete* button at the end of the entry, and choose *Apply*.

More Information

Recording Time for Audit Activities [page 60]

7 Preparation

After an audit is initiated, it goes to the preparation phase, where the audit lead prepares audit announcement letters, if required, designs work program and sends them to the audit manager for review.

When the audit manager approves the work program, the preparation work is finished and the audit is ready to be performed. It moves from the preparation phase to the execution phase.

In this section, you will find information about the following topics:

- Prepare Audits [page 62]
- Review Audit Preparation [page 72]

7.1 Prepare Audits

After an audit is initiated, the audit lead can start to prepare the audit in the app *Prepare Audits*. Preparation of an audit includes the following tasks.

Prepare and submit audit announcement letter (Optional)

An audit announcement letter is a document that contains the basic information about the audit, such as the audit team, the time period and the audit scope engagement.

The audit lead creates an announcement letter and submits it to the audit manager for review, if required. The audit manager approves or rejects the announcement letter, as the case may be, and distributes approved announcement letters to stakeholders when needed.

> i Note
>
> The audit announcement letter and the approval process are optional. It is determined by the audit status schema associated with the audit type. SAP delivers two default audit status schemas: `DEFAULT` and `DFLT_ANN`. Schema `DFLT_ANN` includes the audit announcement letter approval process. You can create your own status schema based on the `DFLT_ANN` schema to enable the process. For more information, see the Customizing activity ▶ *SAP Audit Management* › *Define Audit Status Schema* ◀

If an audit announcement letter and the approval are required, the audit lead must create an announcement letter and achieve approval before he or she can proceed to prepare work program.

Prepare and submit work program

A work program is documentation that contains the methodologies, detailed procedures, and tasks to be performed to achieve the audit objectives.

The audit lead designs the work program and submits to the audit manager for review. The audit manager approves or rejects the work program, as the case may be. A rejected work program needs to be reworked by the audit lead until it is approved.

Related Information

Prepare Audit Announcement Letter [page 63]
Prepare Work Program [page 64]

7.1.1 Prepare Audit Announcement Letter

In the *Prepare Audits* app, you can prepare announcement letters for an audit and submit your announcement letter to the audit manager for review.

Create announcement letter

To create an announcement letter, go to the *Working Paper* section. You can either generate an announcement letter using a template or upload a file as your announcement letter. Announcement letters are put in the *Preparation/B* folder in the *Working Paper* tab .

Generate announcement letter

To generate an audit announcement letter automatically using a predefined file template, choose *Generate* and select a template you want to use.

> i Note
>
> For more information about file templates, see the Customizing activity ▶ *SAP Audit Management* › *Audit Preparation* › *Audit Announcement Letter* › *Maintain Templates for Generating Announcement Letters* ◀.The default PDF template is delivered in English. If you want to generate the announcement letter in other languages, you need to first create a translated version of text object `GRCAUD_ANN_LETTER_NEXT_STEPS` in that language in transaction `SO10`.

Upload announcement letter

You can upload a file as an audit announcement letter. To do this,

click the + button to upload, or just drag and drop the file from your desktop to the *Working Paper* tab.

With the Fiori *Prepare Audits*, you can add new versions of an announcement letter with previous versions preserved.

Submit announcement letters

After an announcement letter is ready, you can submit it for review. To do so, click *Submit Announcement*. The submitted audit announcement letter can then be found in the audit manager's *Approve Audit Preparation* tile.

Related Information

Review Audit Preparation [page 72]

7.1.2 Prepare Work Program

In the *Prepare Audits* app, you can prepare the work program of an audit.

> i Note
>
> Before you prepare the work program for an audit, you need to define its scope schema first. A scope schema determines how many levels of nodes and the scope names that you will use in the structure of your work program. SAP delivers sets of predefined scope schemas with different levels. You can use the standard schemas or create your own.
>
> The default schemas delivered by SAP refer to the different levels of scopes as *key scope*, *scope*, and *work package*. In this documentation, the default names will be used when referring to the work program scopes. If you change the scope names in the Customizing, bear in mind that they are still referred to as the default names in the Application Help.
>
> For more information about scope schema, see the Customizing for SAP Audit Management under: *SAP Customizing Implementation Guide* > *SAP Audit Management* > *Audit Preparation* > *Define Scope Schema for Work Programs*.

To prepare the work program for an audit, select it and go to the *Work Program* section. You are provided with the following optional ways to prepare the work program.

- Choose the *Edit* button to manually enter the work program.
- Use the *Download* and *Upload* buttons to prepare the work program with a spreadsheet tool. For more information, see the next section **Upload work program using spreadsheet**.
- Choose the *Copy* button to copy a work program from an existing audit or from a predefined template. The copy functionality provides you options to replace the entire work program or to extend it with the items from the source.

Upload work program using spreadsheet

You can use the spreadsheet template to prepare your work program offline and upload it to the system.

1. Click the *Download* button to download the spreadsheet work program template.
2. Open the template offline and enter your work program details.
3. Upload the spreadsheet file to *Work Program* using the *Upload* button.

> ⚠ Caution
>
> If a work program already exists, it will be overwritten by the uploaded file.

> i Note
>
> The system does not check any required fields in the work program template. If you forget to fill a field, you can choose *Current Work Program* when you click *Download* to edit the work program offline and upload it again.

For more information about using the template, see Working with Spreadsheet Templates [page 32].

Edit work packages

The next step is to edit the details of the work packages, also known as scopes.

1. Choose a work package/scope to go to its details page.
2. Enter a description and assign a person responsible for the work package.

    > i Note
    >
    > You can only add description for a work package before the work program is approved. However, you can assign responsible persons to work packages as long as the audit is still ongoing. The available responsible person options can be customized in the Customizing activity ▶ *SAP Audit Management* ▶ *Audit Preparation* ▶ *Define Scope Schema for Work Programs* ◀.

3. Add risks and controls that you want this work package to cover.
4. Next, you can create audit procedures you want to this work package to contain. For more information, see Audit Procedures [page 66].

Related Information

Review Audit Preparation [page 72]

7.1.2.1 Audit Procedures

Audit procedures are designed and performed by the auditor to obtain sufficient appropriate audit evidence. An audit procedure can be a test procedure, a questionnaire, or an automatic detection task. In a test procedure, you can specify which controls to be tested and add detailed test steps to test the controls. In a questionnaire, you prepare a list of questions with predefined answers to choose from and an additional comment field. Detection tasks can be added and scheduled to run automatically to find irregularities in business data.

In this section, you can find information about the following topics:

- Create and Edit Audit Procedures [page 66]
- Detection Procedure [page 68]

7.1.2.1.1 Create and Edit Audit Procedures

Audit procedures are created in a work package/scope to help the auditor obtain audit evidence by assessing risks, testing controls, performing questionnaires and checklists, and executing automatic detection runs.

The following types of procedures are available:

- Test procedure
- Question procedure
- Detection procedure

You can create procedures during the preparation of an audit work program, or you can reopen a work program in the execution phase and append new procedures.

Procedure

To create an audit procedure in a work package, go to the *Procedures* section, click + and choose one of the following options:

- Test
- Question
- Detection

For details of detection type procedures, see Detection Tasks [page 68].

1. Enter the following information:

Field/Procedure Type	Test	Detection	Question
Title (Required)	X	X	X
Description (Optional)	X	X	X

Field/Procedure Type	Test	Detection	Question
Planned Start/End Date (Optional)	X		
Responsible Person (Optional)	X		
Weight (Required)			X
Detection Strategy (Required)		X	

2. Click *OK/Create* to save the procedure.
3. The newly created procedure appears as an entry in the *Procedure* section. Now click the procedure to continue to edit the procedure here. For test procedures, you can also add the following additional information:
   - In the *Controls* section, click + to select and add controls that you want to test in this procedure. Note that only those controls that are assigned to this work package can be added.
   - In the *Steps* section, you can manually add test steps to the procedure. If a control is imported from SAP Process Control and contains a test plan, you can also copy the test steps to the procedure.

   In the *Comments* section, you can submit your comments regarding the procedure, which will be seen by other members of your audit team. This enables the team members to exchange information.

Note that you can only add, edit, and delete procedures before the work program is approved.

Uploading Procedures Using Spreadsheet

You can use the work program template to mass create and upload test and question procedures using spreadsheet.

On the *Work Program* tab of the audit, choose *Download Template* to download the work program template. Open the template offline, enter the work packages/scopes in the *Scope* sheet, test procedures in the *Test Procedure* sheet, test steps for each test procedure in the *Test Steps* sheet, and questions in the *Questions* sheet, save and upload the template.

For more information about using the template, see Working with Spreadsheet Templates [page 32].

More Information

Audit Procedures [page 66]

7.1.2.1.2 Question Rating and Weight

SAP Audit Management is capable of automatically calculating scores for question-type audit procedures. The score of a question is obtained by multiplying the rating score and the assigned weight. To enable this, you need to define question ratings in Customizing and assign a weight when you create a question.

Define Question Ratings

For details of defining question ratings, see the IMG documentation under transaction `GRCAUD_IMG` *SAP Audit Management* > *Audit Preparation* > *Define Question Ratings* .

Assign Weight to Questions

When you create a new question, you can set a weight with numeric value from 0 to 100. The score will be automatically calculated when the question is rated and set to completed status during audit execution. By default, the weight is set to 1. In the case of a 0 weight, the question is considered as non-applicable.

> i Note
>
> Weight is only visible in the preparation phase. During execution, you can export the work program to see the weight value.

Related Information

Create and Edit Audit Procedures [page 66]
Perform Audit Procedures [page 76]

7.1.2.1.3 Detection Procedure

Detection procedures are part of the work program of an audit. With a detection procedure, you can harness the power of SAP Business Integrity Screening and its mass detection feature to find irregularities in business data that are relevant to an audit.

In this section, you can find information about the following topics:

- Background Information [page 68]
- Create Detection Procedure [page 71]
- Detection Information [page 71]
- Analyze Alert Items [page 79]
- Perform Detection Procedures [page 79]

7.1.2.1.3.1 Background Information

A detection procedure lets you use SAP Business Integrity Screening detection strategies to find irregularities in the data that you are auditing. Detection procedures let you integrate the detection and investigation capabilities of SAP Business Integrity Screening into SAP Audit Management.

You create a detection procedure in the work program of an audit.

If a detection strategy finds irregularities and generates alert items, then these items populate a working paper that is added to the work package. From the working paper, you can use the investigative and management tools of SAP Business Integrity Screening to analyze each irregularity.

Special Detection Strategies and Alerts for SAP Audit Management

Detection strategies for use in detection procedures have these special features:

- Only detection strategies that have been specially marked for use in SAP Audit Management may be used in detection procedures. These strategies may not be used by SAP Business Integrity Screening for detection.
  This feature ensures that an audit detection strategy produces alert items only in the context of an audit.
- You maintain audit detection strategies using the normal editing tools of SAP Business Integrity Screening. You designate a detection strategy for use in auditing by setting the special *Audit strategies* (technical key `AUDIT` in Customizing) investigation reason when you define the strategy.
- An audit detection strategy may be assigned to only a single detection procedure at a time. If a detection strategy is assigned to a task, then it is removed automatically from the list of strategies in the input help.
- Audit detection strategies are allowed to produce duplicate alerts and alert items. This feature makes it possible for the same alert item to be used in separate audits that may be examining different aspects of a compliance problem.
  Normal detection strategies produce only a single alert per investigation object. Each irregularity that is found is added to this alert as an alert item. For example, each irregularity found in a purchase order item is added as an alert item to a single alert for the purchase order.
  An audit alert is instead associated 1-1 with its work package. Each irregularity that is found is added as an alert item to a working paper in the work package. Audit detection strategies produce no duplicate alert items within a work package. But other detection procedures in other audits may produce the same alert items in the context of their own work packages and audits.
  Changing the status of an audit alert item in one working paper has no effect on any other instances of the alert item in other working papers in the same work package. You can change the status of an audit alert item without worrying that you are changing the status of the item in other audits.

Audit Detection Strategy Control and Execution

Detection procedures are integrated into the lifecycle of an audit. This feature ensures that audit detection strategies can be assigned and executed only at the appropriate phases in the life of an audit.

Detection procedures are integrated into the audit lifecycle as follows:

- You can create or edit a detection procedure only in the audit phases *Initiated* and *Work Program Rejected*. In the *Initiated* phase, you can choose the audit detection strategy to use. In the *Work Program Rejected* phase, you can respond to objections by adding a detection procedure or editing a task to choose a different audit detection strategy.
- An audit detection strategy can be run only in the audit phases *In Execution*, *Final Report Submitted*, and *Final Report Rejected*.

You create and edit strategies for audits in SAP Business Integrity Screening, just as with normal strategies. In SAP Audit Management, you only choose and run detection strategies. These audit detection strategies must have been prepared previously in SAP Business Integrity Screening.

In SAP Audit Management, you are responsible for ensuring that the detection strategy matches your audit. That is, the investigation object type and detection object type match the data that is the subject of the audit. The parameters for selecting data to examine are correct with regard to the audit, and so on. You can display an audit detection strategy from a detection procedure and verify this information. But SAP Audit Management cannot check that the strategy is optimal for the purpose.

Working with detection procedures and Associated Working Papers

Detection procedures let you integrate SAP Business Integrity Screening into your audits in SAP Audit Management. This section describes the process for working with SAP Business Integrity Screening in the context of an audit.

You have started an audit and want to use SAP Business Integrity Screening to examine relevant business data for irregularities. How do you proceed?

1. Start by defining a detection strategy in SAP Business Integrity Screening for use in SAP Audit Management.
   You must define and activate such a strategy for each detection procedure that you create.
   To define such a detection strategy, you use the standard tools of SAP Business Integrity Screening. You set the *Investigation Reason* to specify that the strategy is for use in SAP Audit Management.
   For more information, see Creating Detection Strategies.
2. In SAP Audit Management, create a detection procedure and use it to run the detection strategy. For more information, see Create Detection Procedure [page 71] and Perform Detection Procedures [page 79].
3. Open the working paper that contains the alert items generated by an audit detection strategy.
   What is an alert item? It is a special message issued by SAP Business Integrity Screening. It reports that a detection strategy has found the signature of potential fraud or business irregularity with respect to a particular business record or event.
   If a detection procedure generates alerts of possible fraud when it is run, then these alert items are placed in a working paper. The working paper is created the first time that alert items are generated. The working paper is part of the same work package as the detection procedure.
4. Use the investigative tools of SAP Business Integrity Screening to analyze each alert item in the working paper.
   From an alert item in the working paper, you can navigate to SAP Business Integrity Screening, to the alert details. There, you can determine whether the alert item is confirmed, a false alarm, or closed without investigation. The status, set in SAP Business Integrity Screening, is shown in the working paper in SAP Audit Management.
   For more information, see Investigation.
5. When all of the alert items have been classified, you can decide whether the working paper supports making a finding in the audit on which you are working. For more information, see Findings and Actions [page 80].

7.1.2.1.3.2 Create Detection Procedure

A detection procedure lets you use SAP Business Integrity Screening detection strategies to find irregularities in the data you are auditing. A detection procedure is part of the work program of an audit.

Follow the instructions described below to create a detection procedure. Note that you can only create a detection procedure for audits in status *Initiated* or *Work Program Rejected*.

Create detection procedure

1. Go to the *Procedures* section in a work package and click *Add*.
2. Choose the type *Detection* .
3. Enter title and description, and select a detection strategy.

   > **i** Note
   >
   > You can select only from special detection strategies for SAP Audit Management. Further, detection strategies that are already in use in another detection procedure are not shown here.

4. Click *OK/Create* to save the procedure.

Edit detection procedure

You are allowed to make changes to the title, description or the detection strategy when the audit is in status *Initiated* or *Work Program Rejected*

More Information

Background Information [page 68]

7.1.2.1.3.3 Detection Information

- In a detection procedure, click its detection strategy and you will be directed to the detection strategy in SAP Business Integrity Screening, where you can check or adjust selection and method parameters, calibrate and optimize the strategy, activate the strategy, or make other changes.
- From the link in the *Working Paper* section, you can navigate to the working paper that contains the alerts found by the detection task.
- In the *Automatic Runs* section, you can see how many times a mass detection has been run, using the SAP Business Integrity Screening detection strategy specified in the task. Alerts can be created and inserted into a working paper only if the detection strategy has been run.

If the *Status* column shows that there was an execution error during mass detection, then you can use the log feature of SAP Business Integrity Screening to display the error messages. For more information, see Analyze Mass Detection Log.

7.2 Review Audit Preparation

Use

In the *Approve Audit Preparation* tile, you can:

- Review the announcement letter
- Distribute the announcement letter
- Review the work program

Depending on the audit type, you may have to approve and distribute the announcement letter before the auditor can prepare the work program.

Reviewing the audit announcement letter

After the audit announcement letter is submitted, the audit appears in the *Approve Audit Preparation* tile. As the audit manager, you can review the document and decide to approve or reject it.

If you approve the announcement letter, the audit status becomes *Announcement Approved*. You can distribute the audit announcement letter to the stakeholders in the same tile. If the audit announcement letter approval process is required for this type of audit, the audit lead can submit the work program after the audit announcement letter is distributed.

If you reject the announcement letter, the audit will be sent back to the audit lead for rework.

Distributing the audit announcement letter

After the announcement letter is approved, you can distribute the announcement letter to the stakeholders. To do so:

1. Go to the *Approve Audit Preparation* tile.
2. Open an audit in status *Announcement Approved* and navigate to the *Working Paper* tab.
3. Choose *Distribute*, add optional notes if necessary, and choose *OK*.

Reviewing the work program

After the work program is submitted, the audit appears in the *Approve Audit Preparation* tile. As the audit manager, you can review the submitted work program, make necessary changes, and decide to approve or reject it.

If you approve the work program, the audit status becomes *In Execution*, which means the audit lead and auditors can start the auditing work.

If you reject the work program, the audit will be sent back to the audit lead who prepared the work program. The audit lead finds the rejected audit in *Prepare Audits*, and keeps revising the work program until it is approved.

Work Program Code

Once a work program is approved, the system generates a code for each structure node in this work program. This code is attached to the node name, and can be used for reference purpose. Reference codes for work program structure nodes are generated by appending a two-digit sequential number to the code of the parent object.

When a working paper is created under a node, the reference code for the working paper is also generated by appending a two-digit number after the work program code.

> Example
>
> When you create a three level structure work program, the reference codes for the nodes may be `A-01`, `A-01-01`, and `A-01-01-01`.
>
> When you create working papers under node `A-03-05-12`, the reference code for the working papers start as `A-03-05-12-01`, `A-03-05-12-02`...and so on.

More Information

Prepare Audits [page 62]

8 Execution

After the work program of an audit has been approved, this audit goes to the execution phase with its status changed into *In Execution*. The execution phase is when the actual auditing activities take place. In this phase, auditors conduct interviews, gather information, collect evidences, record findings and make conclusions and recommendations.

Related Information

Document Your Audit Work [page 74]
Process Work Packages Offline [page 75]
Perform Audit Procedures [page 76]
Perform Detection Procedures [page 79]
Analyze Alert Items [page 79]
Reopen Work Program [page 74]
Findings and Actions [page 80]

8.1 Reopen Work Program

You are allowed to reopen the work program of an audit in status *In Execution* to revise the work program.

To do this, click the *Reopen Work Program* button. The audit then changes to status *Work Program Reopened* and can be accessed in *Prepare Audits*.

As an audit lead, you can modify the work program and submit it again for review and approval.

> **i Note**
>
> You can only add new work packages to the work program. Editing of existing work packages is not allowed, nor is uploading work program using spreadsheets.

8.2 Document Your Audit Work

You can document the audit work you have completed for each work package in the work program. This information is saved as notes attached to the work packages.

To document your audit work:

1. Find this audit in *My Ongoing Audits*, and navigate to the *Work Program* section and open a work package .
2. Choose the *Work Done*/*Work Done Notes* button, and type your notes.
3. After you finish, choose *OK* to save the notes.

After saving the notes, you can choose the *Work Done*/*Work Done Notes* button again to review and edit the text. The notes will be visible to all users who have access to this audit.

If you process your work package offline, you can also enter your work done notes in a PDF file and send it back to the system. For more information, see Processing Work Packages Offline [page 75].

8.3 Process Work Packages Offline

You can process audit work packages assigned to you using SAP Interactive Forms by Adobe. This offline processing feature enables you to perform your audit work without having to log on to the SAP Audit Management system. With SAP Interactive Forms by Adobe, you can enter work done notes, attach working papers to a PDF document, and send them back to the system via e-mail.

Prerequisites

- A virtual host to the SMTP server has been created in your client with SAP Audit Management power user information maintained on the logon data tab. Contact your system administrator to create the virtual host. For more information, see the Online Manual under transaction `SICF`.
- You have installed and configured the Adobe Document Service (ADS). For more information, see the *Installation Guide* for SAP Assurance and Compliance Software at http://help.sap.com/audit .
- You have installed a PDF software that supports XFA (XML Forms Architecture) content.
- You have completed the relevant Customizing settings in the following activities:
  - *Maintain Templates for File Generation*
  - *Maintain E-mail Notifications for Audit Activities*

  For more information, see the documentation for the respective Customizing activities.

Procedure

1. Go to an initiated audit, prepare the work program, assign responsible persons to work packages, and submit the work program.
   After the audit manager approves the work program, individual work packages are sent to their responsible persons as PDF attachments to the notification e-mails.
2. As a responsible person for the work package, you open the PDF file in your e-mail and perform your audit as described in the work package.
3. If JavaScript is disabled in the PDF document, enable it.
4. To add working papers to the work package, click on the *Attachments* tab on the side panel, choose *Add*, select the files, and choose *Open*.

5. You can also enter your work done notes in the *Notes* field.
6. After you finish processing the work package, send the PDF document back to the system using one of the following methods:
   ○ If you are using an e-mail client, choose the *Submit* button in the PDF document. A reply e-mail window opens with the updated PDF document attached. Send the e-mail back to the system.
   ○ If you are using a web browser, save the PDF document from the e-mail, attach it in the reply to the notification you have received, and send it back to the system.

   > i Note
   >
   > Do not use the default recipient address when you send the reply. The correct recipient address can be found in the configuration of the exit rule for inbound processing under transaction `SO50`. Use the recipient address corresponding to exit name `CL_GRCAUD_EMAIL_INBOUND`.

If the e-mail is received successfully, the attachments and notes appear under the work package in SAP Audit Management.

For more information about the offline processing feature, see Extending the Offline Processing Featurein the *SAP Audit Management Extensibility Guide*.

More Information

Prepare Audits [page 62]

8.4 Perform Audit Procedures

After the work program is approved, the auditors can find this audit in the app *My Ongoing Audits* with the status *In Execution* and start the execution of the audit by performing the audit procedures contained in the work packages/scopes.

For test procedures, you can set the control effectiveness after testing, add working papers, report findings and document the conclusions from performing the audit procedure. For question procedures, you can provide answers and comments, add working papers and record your findings.

Test procedure

In the *Procedures* section, select a test procedure and perform the following tasks.

Conclusion

In the *General* section, click the *Edit* icon to enter your conclusions of performing the audit procedure.

Control Effectiveness

In the *Controls* section, set the effectiveness result for a control as follows:

1. Click the *Set Control Effectiveness* button.
2. Select an effectiveness result from the drop-down list in the *Effectiveness* field.

   > i Note
   >
   > The effectiveness settings can be defined in the Customizing activity under `GRCAUD_IMG` ▶ *Master Data* ▶ *Controls* ▶ *Maintain Control Effectiveness Settings* ◀.

3. Optionally, you can also enter comments for the control testing.

Working Papers

In the *Working Papers* section, you can add working papers to the test procedure by uploading new working papers or adding existing ones. To add an existing working paper, choose *Select*.

Findings

If you have findings relevant to this test procedure to report, you can add them in the *Findings* section. To do this, you can create a new finding or assign an existing one.

When you finish, you can set the test procedure to *Completed*by clicking the *Complete* button.

Question procedure

In the *Procedures* section, select a question procedure and perform the following tasks.

1. In the *Question* section, click the *Edit* button and select an answer for the question from the available choices. You can type some comments if you want.
2. In the *Working Papers* section, upload or assign existing working papers that you want to add to this question procedure.
3. If you have findings relevant to this question procedure to report, you can add them in the *Findings* section. To do this, you can create a new finding or assign an existing one.

> i Note
>
> For information about calculating the score of a question procedure, seeCalculating Question Scores [page 78]

When you finish, you can set the test procedure to *Completed*by clicking the *Complete* button.

Detection procedure

For instructions on running a detection procedure, seePerform Detection Procedures [page 79].

Reopen audit procedures

You can reopen a completed procedure if you need to make modifications before the final audit report is approved.

More Information

Audit Procedures [page 66]

8.4.1 Calculating Question Scores

Scores are calculated automatically by multiplying the question rating and its assigned weight. Scores can be obtained on the scope level by aggregating all questions under the scope, and on the audit level by aggregating the scores of all the scopes.

If a question rating or weight is set to 0, then the question is considered as non-applicable (NA) and does not count in the final scores.

Example

Audit 2016-001 has four rating defined in Customizing: 3, 2, 1, and 0 (NA). Below is an example of how its scores are calculated based on rating and weight.

Scope	Question	Rating	Weight	Weighted Score	Scope Score	Audit Score
Scope A	Question A-1	1	1	1	Actual score: 4 Maximum score: 6 Overall score: 4/6 (66.67%)	Final audit score: 12/15 (80.00%)
	Question A-2	2	0	0		
	Question A-3	3	1	3		
Scope B	Question B-1	2	1	2	Actual score: 8 Maximum score: 9 Overall score: 8/9 (88.89%)	
	Question B-2	3	2	6		
	Question B-3	0	2	0		

Related Information

Question Rating and Weight [page 67]

8.4.2 Perform Detection Procedures

Running a detection procedure helps you find out whether any irregularities exist in the business data that you are auditing. When irregularities are identified through running a detection procedure based on the detection strategy, these irregularities are recorded as alert items in a working paper of the detection procedure.

Note that you can run a detection procedure only when the audit is in one of the following statuses:

- *In Execution*
- *Final Report Submitted*
- *Final Report Rejected*.

Run detection procedure

1. Find the detection procedure you want to run in the *Procedures* section and click it.
   The details page of the detection procedure shows information about the procedure including its status, the detection strategy employed, related working papers, if any, and whether the procedure has been run before. You can click the detection strategy to see its details and verify that the selection and detection method parameters are correct.
2. Click *Run* to run the detection procedure. SAP Business Integrity Screening uses the detection strategy assigned to the task to perform mass detection.

   Each run is recorded as an entry in the *Automatic Runs* tab. You can click ↻ on the top-right of the tab to get the current status of the runs you have launched.
   Following the completion of the first run of a detection procedure, a working paper is automatically generated, which can be found in the *Working Papers* section. Any irregularities found during each run are recorded as alert items in the working paper. No duplicate alert items will be created. Alerts are automatically assigned to the user who is responsible for the work package.

   > i Note
   >
   > If an error occurs during a run and is reported, you can use the SAP Business Integrity Screening log transactions to display the error log produced. For more information, see Analyze Mass Detection Log. You can also use the debugging facilities offered by SAP Business Integrity Screening. For more information, see Testing and Debugging Detection Strategies in Simulated Mass Detection Runs.

8.4.2.1 Analyze Alert Items

Issues or irregularities found by performing a detection procedure are recorded as alert items in the working paper of this procedure.

This section explains how to analyze and classify these alerts.

Process

1. The working paper lists the alert items generated by each run of the detection procedure. The columns of the tables have the following meanings:
   - The first column identifies the business entity with respect to which an irregularity was discovered. This business entity may be, for example, a vendor, a purchase order, or an insurance claim. All alert items in a working paper pertain to the same type of business entity.
   - The *Additional ID* columns provide more information on the business entity, such as the name of a vendor or the number of a purchase order item. The contents of these fields are tailored to the type of business entity.
   - The *Additional Date* field shows the date of the business irregularity. The date may be the posting date of a suspicious purchase order or the date on which a suspicious vendor master data change occurred.
   - The *Status* field shows the status of the alert item, as shown in the *Finding*. The status may be, for example, *Confirmed* or *Closed Without Investigation*. You can set the status only in SAP Business Integrity Screening, on the *Decision* tab in the alert item details.
2. Click an alert item to open the alert in SAP Business Integrity Screening. From the alert, you can navigate to the alert item. You can use the investigative tools of SAP Business Integrity Screening to analyze the alert item, document your work, and set the status in the *Finding* field. For more information, see Investigation.

When you have set a finding for each alert item in the working paper, you can then determine whether a finding in the audit is required.

8.5 Findings and Actions

Findings are the result of the auditing process that evaluates the audit evidence and compares it against the audit criteria. In a finding, the auditor documents any errors, deficiencies, or adverse conditions identified during auditing. A finding is usually accompanied by **recommendation** for counteractive measures and an **action plan** to address the issues.

You can create new findings and access existing findings of an audit in the *Finding* section.

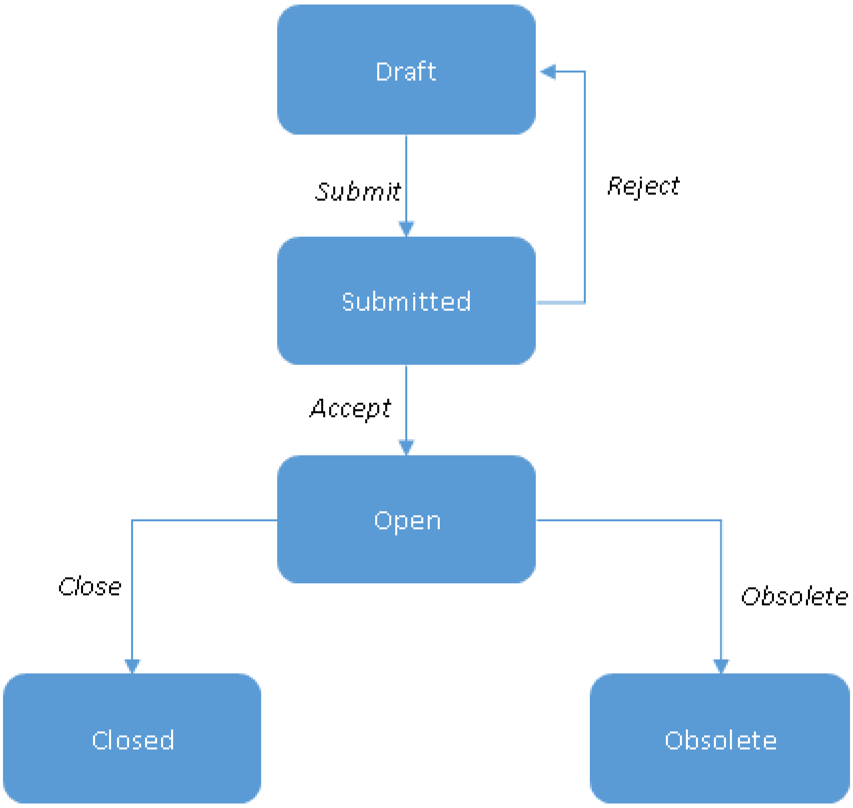
Finding Status

A finding has one of the following statuses:

Status	Description
Draft	When a finding is created, it has the status *Draft*.

Status	Description
Submitted	After a finding is submitted to the auditee for review, the status becomes *Submitted*.
Open	When a draft finding becomes an open finding, you can view it in *Track Open Findings* and evaluate how the management has responded to the recommendations and actions proposed in the finding.
Closed	You can close a finding when the actions in the finding have been completed, or when the management accepts the risks of not taking them.
Obsolete	You can change the status of a finding to *Obsolete* when the content of the finding and the actions become irrelevant.

The figure below illustrates the status change of a finding:



More Information

Findings [page 82]

Action Plans [page 84]

Tracking Open Findings [page 93]

Tracking Open Actions [page 95]

8.5.1 Findings

You can only create findings for an audit in status *In Execution*, *Rework Draft Report*, or *Rework Final Report*. You can create as many findings as you need for one audit.

To create a new finding, click + on the top-right of the *Findings* section and enter the following information.

Field	Required/Optional	Description
Title	Required	Title of the finding, maximum length is 80 characters.
Description	Optional	Enter a description of the finding here.
Type	Required	A risk classification for the findings, which defines the risk area impacted by this finding. Examples of finding types are: Economic, Financial, Market, or Operational.
Category	Required	A sorting classification for reporting purposes. Examples of find categories are: Board- and Non-Board Relevant.
Ranking	Required	Used to classify the risk in values, in order to prioritize the actions to undertake for the mitigation of the risk. Examples of finding rankings are high, medium, and low.
Executive Responsible	Optional	Select one executive responsible from the drop-down list. Responsible persons are assigned to the audit when it is created.
Reference	Optional	Select an entry from the list of work program scopes as a reference for the finding.
Status	Required	The different stages of a finding. The finding status is automatically set as *Draft* upon creation.

Field	Required/Optional	Description
Tags	Optional	A flag or label you can use to be able to easily search for the finding with the search tool. Enter whatever phrases you like; the field is a free-text field. Note: To save your tag, you must choose the + (*Add*) icon after making your entry.

Field	Required/Optional	Description
Criteria	Required	The standards, measures, expectations, policies, or procedures that should be complied with. The criteria explain “what should be”.
Condition	Required	The factual evidence that the auditor found in the course of the examination. The condition explains “what is or has happened”.
Cause	Required	The reason the condition occurred. The cause is the difference between what-is (condition) and what-should-be (criteria).
Consequence	Required	The effect or what can happen as a result of the current condition.

> i Note
>
> For more information about finding type, category, and ranking, see Customizing for SAP Audit Management under ▶ *SAP Audit Management* › *Audit Execution* › *Document Findings, Recommendations, and Actions* ◀.

Recommendation

You can type your recommendation such as suggested corrective measures for the auditee.

Working papers

You can assign working papers that already exist and have been added to the audit to the finding. Note that you cannot create a new working paper here.

Controls

If the finding is related to one or more controls that have been tested during the audit, you can link the finding to these controls.

Action plans

Actions are the result of the communication between the auditor and the auditee with respect to the finding. They reflect how the auditee plans to correct the findings and implement the recommendations. For more information about actions, see Action Plans [page 84]

Edit and delete finding

You can edit a finding when it is in status *Draft* or *Open*.

Only findings in status *Draft* can be deleted. When you delete a finding, all action plans under the finding are also deleted and the finding is permanently removed from the system.

> i Note
>
> After a finding is successfully created, the system generates an ID for it. You can use this ID for reference purpose. You can also change the pattern of how the ID is generated. For more information, see the *Installation Guide* at http://help.sap.com/audit.
>
> On the finding list, you can also change the ID of findings by adjusting their sequence numbers in edit mode. The sequence number corresponds to the last digits of the finding ID. You can change the ID of any finding in draft status. If there are actions under the finding, the part of the action ID inherited from its parent also changes with the finding ID.

More Information

Findings and Actions [page 80]

Action Plans [page 84]

Tracking Open Findings [page 93]

8.5.2 Action Plans

Use

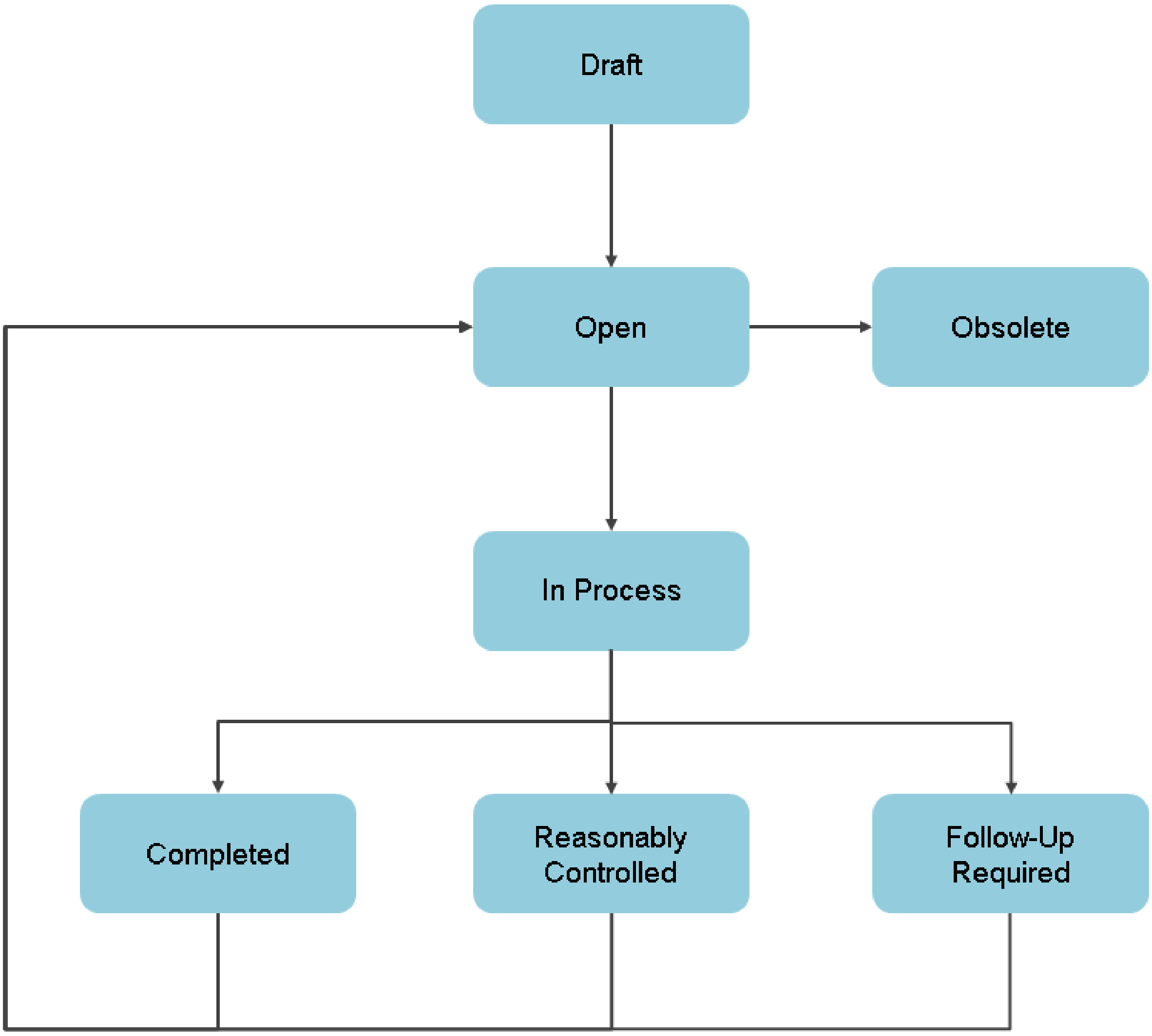
When a finding has been created, you can add actions in the *Action Plans* section of the finding. Actions are the result of the communication between the auditor and the auditee with respect to the finding. They reflect how the auditee plans to correct the findings and implement the recommendations.

SAP Audit Management allows you to create a two-level action plan by default, which means for each action, you can add child actions.

With the default action status schema delivered by SAP Audit Management, an action has one of the following statuses:

Status	Meaning
Draft	An action is marked *Draft* when it is created.

Status	Meaning
Open	When the final audit report is approved, all draft actions under the audit become *Open*.
In Process	The action responsible person responds to their assigned action by setting its status to *In Process*.
Completed	When an action is completed by the person responsible, the action can be set to *Completed*.
Reasonably Controlled	This status indicates that the issue stated in the action plan has been reasonably controlled by the action responsible person.
Follow-Up Required	This status indicates that a follow-up audit is necessary after reviewing the response to the action from the person.
Obsolete	When you obsolete a finding, all actions under the finding become *Obsolete*.



Action Life Cycle

Create action

> **i Note**
>
> Before you create an action, you may want to define the action types first. Do this in Customizing activity *Define Action Type*.

To create an action,

1. Go to the *Action Plans* section and click **+**.
2. Enter the following information.

Field	Optional/Mandatory	Description
Title	Mandatory	Name of the action.
Type	Mandatory	Select the action type.
Action Plan Responsible	Mandatory	Appoint one or more persons to be responsible for performing the action. When the final report is approved for the audit, the responsible persons receive an e-mail with the action details attached.
Description	Optional	Describe the details of the action.
Deadline	Mandatory	Set a deadline for the person responsible to complete the action.

3. Save.
4. To create child actions for the action you have just created, select it and scroll down to the *Action Plan* section.

Edit and delete action

Actions can only be edited and deleted when they are in *Draft* status.

In the *Action Plans* section, you can also change the ID of actions by adjusting their sequence numbers in edit mode. The sequence number corresponds to the last digits of the action ID. You can change the ID of any action in draft status. If there are child actions, the part of the action ID inherited from its parent also changes with the parent action ID.

More Information

Tracking Open Actions [page 95]

Findings [page 82]

8.5.3 Communicating Audit Findings with the Auditee

Use

As an auditor, you can communicate the conclusions to the auditee to reach an agreement on the audit findings and the follow-up action plans. After the auditee acknowledges the audit findings and understands that the evidence of the reported nonconformity or noncompliance is accurate, you can set the findings and action plans to open for follow-up.

The interaction between the auditor and the auditee is based on the finding approval process. As an auditor, you can submit a draft finding to the auditee for review. The auditee receives a PDF form with the finding details and decides whether to accept or reject the finding. The auditee can also enter optional notes, such as action plan proposals, and send them back to the system.

After the auditee accepts a finding, the status of the finding and its action plans changes to open. You can find the open findings in the *Track Open Findings* and *Track Open Actions* tiles.

More Information

Tracking Open Findings [page 93]

Tracking Open Actions [page 95]

9 Reporting

Reporting is the final phase of the audit. During the reporting phase, auditors prepare draft and final audit reports and send them to the audit manager for review. Final reports can only be submitted for review after the draft report has been approved by the audit manager. Approved final reports can be issued to stakeholders to communicate the audit objectives, audit scope, conclusions, recommendations, and action plans.

In this section, the following topics are covered:

- Prepare Audit Reports [page 89]
- Review Audit Reports [page 90]
- Issue Audit Reports [page 91]
- Close Audits [page 91]

9.1 Prepare Audit Reports

As an audit lead, you create audit reports and submit them to the audit manager for review in *My Ongoing Audits*. You can create audit reports for audits with one of the following statuses:

- In Execution
- Draft Report Approved
- Rework Draft Report
- Rework Final Report

Create audit reports

You can create an audit report by uploading a local file or by generating it online using report templates.

Upload audit reports

To upload a local file, go to the *Report* section and click +. Drag-and-drop uploading is also supported, except in Internet Explorer.

Generate audit reports online

You can generate an audit report online using audit report templates. To do this, click *Generate*, choose a category and a rating, enter the executive summary and select a report template.

> ℹ Note
>
> Before you start, complete the configuration settings in the Customizing activity *Maintain Templates for Generating Audit Reports*.

Edit and delete audit reports

You can edit the name of an audit report and delete a report before it is submitted for review.

Submit audit reports

If you are the audit lead, you can send the audit report to the audit manager for review by choosing the *Submit Draft Report* or *Submit Final Report* button as the case may be.

You can only submit the final report after the draft report is approved.

More Information

Review Audit Reports [page 90]

9.2 Review Audit Reports

As an audit manager, you review the audit report submitted to you in *Approve Audit Reports* and choose to approve or reject it. You can type your review notes for the reports.

After you approve a draft report, the audit lead can proceed to prepare the final report and submit it for review. An approved final report can be issued publicly to the stakeholders. You then have the option to track open findings and close the audit.

When you reject a draft or final report, it will be sent back to the audit lead for rework. The audit lead can modify the report and submit it again for review.

If e-mail notification is enabled, you can also receive an e-mail with the audit report attached as a PDF or Word document. In the case of draft report, a PDF approval form can also be attached. You can approve or reject the report directly within the PDF form.

Interactive Audit Reports

When generating audit reports, you can choose a template of the *IDOC - Interactive Audit Report* type to generate an interactive audit report. This type of Word report allows you to modify audit information directly in the document and apply the changes in the system.

To review the content of an interactive audit report, download the document online or from your e-mail, modify the fields where needed, save your document, and upload or send it back to the system via e-mail. You can modify the following fields:

- Executive summary
- Findings, including title, criteria, condition, cause, consequence, and recommendation fields
- Action plans, including action name, action responsible, details, and deadline fields

> ℹ Note
>
> You cannot create new findings or actions, or modify the ID of existing findings and actions in the document. Any changes must be entered in the highlighted grey area.

As an audit lead, you can apply the changes in the audit report to the system by synchronizing the data. To do so, open the audit report in *My Ongoing Audits* and choose *Sync*. Note that the *Sync* button is only available for interactive audit reports.

More Information

Prepare Audit Reports [page 89]

9.3 Issue Audit Reports

Use

After a final report is approved, the audit manager communicates the audit objectives and scope as well as conclusions, recommendations, and action plans to the relevant stakeholders by issuing the final report.

You can go to the *Issue Audit Reports* tile and find a list of audits for which the audit report can be issued. To issue the audit report for an audit, go to the *Report* tab and choose *Issue Report*. The document approved as the final report is sent to the recipients through e-mail.

After you issue the audit report for an audit, the status of the audit becomes *Final Report Issued* and the audit can be closed.

More Information

Prepare Audit Reports [page 89]

9.4 Close Audits

You can close an audit after the final report is issued. A closed audit is read-only and no longer appears on in *My Ongoing Audits* or *Track Ongoing Audits*. You can find all closed audits in *Display Historical Audits*.

To close an audit, find it in *Track Ongoing Audits* and choose *Close*.

> i Note
>
> Only the user assigned as CAE or the audit manager can close the audit.

You can still track the findings and actions under a closed audit. For more information, see Tracking Open Findings [page 93]and Tracking Open Actions [page 95].

10 Follow-Up

In the follow-up phase, auditors evaluate the adequacy, effectiveness, and the timelines of actions taken by management on reported findings and recommendations. In reviewing the evaluation result, the auditor determines whether management has implemented the recommendations or accepted the risk of not implementing them.

The following topics are covered in this phase:Tracking Open Findings [page 93]Tracking Open Action Plans [page 95]Historical Action Plans [page 97]Fiori App: Display Historical Findings [page 98]Communicating with Auditees [page 99]

Exporting Action Plans

The export function in the action list screen allows you to export and download the complete list of open or historical actions. This facilitates the tracking of action plans offline, for example, using a spreadsheet tool.

To enable this function, you need to first maintain the file templates in scenario `LST_ACTION` in Customizing activity under `GRCAUD` ▶ *SAP Audit Management* ▶ *Basic Settings* ▶ *File Generation* ▶ *Maintain Templates for File Generation* ◀. This scenario is offered in the default setting.

To export the action list, click the *Export* icon on top of the action list and choose the desired export format.

The export button is available in *Track Open Actions* and *Display Historical Actions*.

> i Note
>
> The exported document contains the complete list of actions and all information available to the actions, regardless of the personalization and filters applied to the list.

10.1 Tracking Open Findings

After a finding is accepted by the auditee, or after the final report is approved, all findings under the audit are automatically set to status *Open*. All action plans under the findings are also automatically set to status *Open*. You can find all open findings in the *Track Open Findings* tile. This tile allows you to evaluate how the management has responded to the action plans and recommendations proposed in the finding, and decide to either close the finding or obsolete it.

In *Track Open Findings*, you can:

- Close findings
- Obsolete findings
- Add attachments to findings and change executive responsible

- Raising findings as ad-hoc issues
- Complete action plans
- Create new action plans

> i Note
>
> You have to enable this functionality in Customizing activity *Create Action Plans in Follow-Up Phase*.

Closing a finding

You can close a finding when all action plans under the finding are completed. A closed finding is removed from the *Track Open Findings* screen. You can find it under the relevant audit in the *Display Historical Audits* tile.

To close a finding, go to the *Track Open Findings* tile, select a finding, and choose *Close*.

Obsoleting a finding

Under certain circumstances, a finding may no longer be relevant to the audit. In this case, you have the option to obsolete it. When you obsolete a finding, action plans under this finding with status *In Process* are set to *Obsolete*. However, this does not change the status of completed action plans.

To obsolete a finding, go to the *Track Open Findings* tile, select a finding, and choose *Obsolete*.

Completing an action plan

Actions must be completed before a finding can be closed.

To complete an action plan, go to the *Track Open Actions* tile, select an action plan, and choose *Complete*. For more information, see Tracking Open Actions [page 95].

Raise finding as an issue

With a predefined connector, you can raise a finding as an ad hoc issue to SAP Process Control.

To do this, go to the finding display page, choose the *Raise Issue* button, select a connector, and choose OK. Note that you can only raise one issue per finding. Ad hoc issues can be accessed in the *Ad Hoc Tasks* section of *My Home* work center in Process Control.

Creating new action plans

If required, you can also create new action plans for an open finding. Action plans created in *Track Open Findings* need to be manually accepted by auditors. Open the draft action plan and choose *Accept* to set the status to *Open*.

For more information, see Action Plans [page 84].

Related Information

Findings and Actions [page 80]

10.1.1 Fiori App: Track Open Findings

With the transactional app *Track Open Findings* you can track and change the status of open findings, and upload attachments to findings.

Key Features

- Display a list of open findings
- Display the details of the finding and the related action plans
- Change the details and status of findings
- Attach files to findings
- Create new action plans

Related Information

Fiori App: Display Historical Findings [page 98]

10.2 Tracking Open Action Plans

On the *Track Open Action Plans* screen, you can find actions in status *Open* and *In Process*. Open action plans can be set to *In Process* by auditors or the responsible persons. When an action plan is in process, the responsible person can respond to it by sending updates through e-mail. The auditor evaluates the response and decides to set the action plan status to *Reasonably Controlled*, *Follow-Up Required*, or *Completed*.

If you want to close a finding, you must first complete all open action plans under the finding. If you obsolete a finding, action plans under the finding with status *In Process* are also obsoleted.

For more information about action plan status change, see Action Plans [page 84].

Responding to action plans

When a parent finding is accepted by the auditee or when the final audit report is approved, the status of all action plans automatically change from *Draft* to *Open*. The responsible persons of each action plan receive a notification e-mail with details in an attached PDF document. The PDF document also provides the following options for the responsible persons:

- Set the status to *In Process*
- Provide written response in a note

The responsible person selects one of the above options and sends the PDF document back to the system via e-mail by choosing *Submit*.

> **i Note**
>
> You must use the same email account to receive and send the document. By default, email addresses are case sensitive in SAP Audit Management. That means if you maintain email address `abc@sap.com` in your user's master data, you are not able to send back documents to the system using `ABC@sap.com` even if your email client does not differentiate the two addresses. You can toggle the case sensitivity setting in Customizing activity *Maintain Case Sensitivity Setting*.

Extending the deadline and changing responsible persons

When the responsibility of an action plan is shifted and the auditee requires more time to follow up, you may need to modify the responsible persons and extend the deadline of the action plan. You can do so by editing the action plan in *Tracking Open Action Plans*.

Escalating actions

When an action plan is long overdue or requires attention from the management, you can escalate it by clicking the *Escalate* button. All action plans that are open and in process can be escalated. You can escalate an action plan to multiple levels. The escalation level information is maintained in Customizing activity under `GRCAUD_IMG` ▶ *Follow-Up* ▶ *Maintain Escalation Levels for Action Plans* ▶.

> **i Note**
>
> Escalation of action plans does not change their status. You can still find the escalated action plans in *Track Open Action Plans*.

More Information

Tracking Open Findings [page 93]

10.2.1 Fiori App: Track Open Action Plans

With the transactional app *Track Open Action Plans*, you can display a list of open action plans, check and change the status and details of the action plans, and leave comments.

Key Features

- Display a list of open action plans in the system
- Change status of action plans
- Change the deadline and responsible persons of action plans
- Escalate action plans
- Leave comments

Related Information

Fiori App: Display Historical Action Plans [page 97]

10.3 Historical Action Plans

Historical action plans can have the following statuses:

- Completed
- Reasonably Controlled
- Follow-Up Required
- Obsolete

Historical action plans provide information about the management response to the action plans communicated in the audit result. Internal auditors can use this information to decide whether follow-up audits are required.

You can access all historical action plans from the *Display Historical Action Plans*.

Related Information

Fiori App: Display Historical Action Plans [page 97]
Reopening Action Plans [page 98]

10.3.1 Fiori App: Display Historical Action Plans

With transactional app *Display Historical Action Plans*, you can display an overview and detailed information of all historical action plans you're authorized to see. You can also reopen an action plan if additional effort from the auditee is required.

Key Features

- Display a list of historical action plans in the system
- Search, filter, and group the list and save the results as a variant
- Export the list to a spreadsheet
- Reopen a historical action plan

Related Information

Reopening Action Plans [page 98]

10.3.2 Reopening Action Plans

You can reopen a historical action plan if necessary. Action plans in status *Completed*, *Reasonably Controlled*, and *Follow-Up Required* can be reopened at any time.

To reopen a historical action plan, go to *Display Historical Action Plans*, select an action from the list, and choose *Reopen*. Reopened actions can be found in *Track Open Action Plans*.

Related Information

Fiori App: Display Historical Action Plans [page 97]

10.4 Fiori App: Display Historical Findings

With the transactional app *Display Historical Findings*, you can display an overview list as well as detailed information of all closed and obsolete findings which you have access to. You can also navigate to and check the status of the action plans linked to the finding.

Key Features

- Display a list of historical findings in the system
- Search, filter, and group the list and save the results as a variant
- Export the list to a spreadsheet
- Display the details of the finding and the related action plans
- Reopen findings

Related Information

Historical Action Plans [page 97]

10.4.1 Reopening Findings

In the *Display Historical Findings* Fiori app, you can reopen a historical finding. This allows auditors and auditees to continue work on unfinished issues by adding more action plans. You can find reopened findings in *Track Open Findings*.

Related Information

Fiori App: Track Open Findings [page 95]
Fiori App: Display Historical Findings [page 98]

10.5 Communicating with Auditees

Auditors can communicate internal audit results with auditees online. With the **My Findings** and **My Action Plans** Fiori apps, auditees can review submitted audit findings, propose action plans, and monitor the execution status of action plans.

Related Information

Fiori App: My Findings [page 99]
Fiori App: My Action Plans [page 100]

10.5.1 Fiori App: My Findings

With the transactional app **My Findings**, you can display an overview list of audit findings and the detailed information under your responsibility. You can review findings submitted by auditors, propose action plans, and monitor the action plan status.

Key Features

- Display a list of submitted, open, closed, and obsolete findings
- Search, filter, and group the list and save the results as a variant
- Display the details of the finding and the related action plans

- Accept or reject a finding, propose action plans, and assign action plan responsible persons

Related Information

Fiori App: My Action Plans [page 100]

10.5.2 Fiori App: My Action Plans

With the transactional app **My Action Plans**, you can display an overview list of action plans as well as detailed information under your responsibility. You can upload attachments, enter comments, and change status of action plans.

Key Features

- Display a list of open and historical action plans
- Search, filter, and group the list and save the results as a variant
- Navigate to the related findings
- Upload attachments and enter comments
- Complete and reopen action plans

Related Information

Fiori App: My Findings [page 99]

11 Manage Working Papers

Use

Working papers are documents prepared by the auditor to provide a clear understanding of the work performed, the audit evidence obtained and its source, and the conclusions reached. For example, when you create a finding, you can add working papers to provide information that supports your finding substantiate audit results. Working papers can be reviewed by audit managers, audit leads, and other auditors.

SAP Audit Management provides the following features for managing your working papers:

- Create and delete working papers
- Upload and download working papers
- Review working papers with comments

The integration with SAP Business Integrity Screening allows you to use the detection strategies to add detection procedures to work packages, schedule automatic runs, and generate detection working papers. For more information, see Detection Procedure [page 68].

Working Paper Categories

Working papers are categorized and stored in different folders in the *Working Paper* section of an audit. SAP Audit Management delivers the following four folders with each corresponding to a phase of an audit. Working papers created in a specific phase are put in the corresponding folder.

- A – Planning
- B – Preparation
- C – Execution
- D – Reporting

You might see different numbers of folders under audits depending on the audit status.

> i Note
>
> You can configure which folders are accessible to audits with which statuses via Customizing activity *Define Audit Status Schema*, and change the folder names or create your own folders in Customizing activity *Maintain Working Papers Categories*.

Related Information

Create, Edit and Delete Working Papers [page 102]

Reviewing Working Papers [page 103]

Manage Working Paper Versions [page 104]

11.1 Create, Edit and Delete Working Papers

Working papers can be added to any audit except closed audits and canceled audits.

The *Working Papers* section has the following columns:

- Type: An icon indicating the file type of the working paper.
- Code: Once successfully uploaded, the system automatically generates a reference code for the working paper.
- Name: The name of the working paper.
- Last Updated: The user who last updated the working paper and the time.
- Review: The review information of the working paper.

How do I create working papers?

You have several ways to create working papers for an audit.

- Generally, you can go to the *Working Papers* section on the audit page and select the right folder and create working papers.
- Depending on the status of the audit, you can create working papers in specific scenarios.
  Example
  - For an audit in execution, you can create working papers for a specific procedure in the *Work Program* section. If you have a detection procedure, and when you run it, a working paper will be automatically generated as a result. For more information, see Running a Detection Task [page 79]
  - To create audit reports, you can just do that in the *Report* section.
- If you are processing your work package offline, you can add working papers to the work package by attaching them in the PDF document and sending them back to the system. For more information, see Processing Work Packages Offline [page 75].

> i Note
>
> Alternatively, you can assign a file generation scenario to a working paper category and use the templates defined in that scenario to generate working papers online. For more information, see Customizing activity *Maintain Working Paper Categories*.

Edit and delete working papers

After working papers are created, you can edit the name of the working papers, or delete them.

> i Note
>
> You cannot delete a working paper that is already assigned to a finding.

Editing Working Papers Online

You can edit working papers online using editing tools installed on your desktop and save the changes directly in the system.

Select a working paper and choose *Online Edit*. An application is launched to edit the document. Make your changes and save the document. The working paper is automatically updated online. Click the *Refresh* icon in the *Downloads* section to see the *Last Updated* information.

Online editing of the following file formats is supported:

- Spreadsheets (.xlsx, .xls)
- Word documents (.docx, .doc)
- Slide show presentations (.pptx, .ppt)

> i Note
>
> Online editing of working papers only works on the default client of your SAP Audit Management system. It may not work if the front end and the back end are deployed separately.

More Information

Managing Working Papers [page 101]

11.2 Reviewing Working Papers

Use

When a working paper is created, authorized users can review it and enter review notes.

> i Note
>
> Detection working papers are automatically generated as the result of running detection procedures. You cannot enter any review notes to a detection working paper. For more information, see Perform Detection Procedures [page 79].

Review notes can be created, deleted and cleared.

- To enter a review note for a working paper, open the working paper, go to *Review Notes* and choose +.
- To delete a review note, click the *Edit* icon button and choose *Delete*. Note that you cannot delete review notes entered by other users.
- You can enter as many review notes as you need. When a review note is entered, it is marked as *New note*. You can click the note status icon to clear the note. Clearing a review note does not remove it from the working paper. On the working paper list, you can see the numbers of cleared notes and all notes under a working paper.

You can also download and review all working papers in an audit, a scope, an entire work program, or a folder using the *Download all working papers* button on the *Working Paper* tab. The working papers will be downloaded in a zip file.

More Information

Creating, Editing, and Deleting Working Papers [page 102]

Managing Working Papers [page 101]

11.3 Manage Working Paper Versions

If the version management option is enabled for working papers, you can create versions of a working paper, audit report, or other audit documents.

To create new versions of a document, simply upload a document with the same file name. Note that if the content of the new document is the same as the existing one, the system does not create a new version.

You can enable this functionality in Customizing activity *Enable Version Management for Audit Documents*. Once enabled, you can create versions of documents in the entire system. You can also disable the functionality, but the versions of existing documents can still be accessed.

12 Data Protection

The following functions support you in handling personal data as well as archiving and deleting data.

- **Display Personal Data**
- **Logging Changes to Personal Data**
- *Remove User Names* (transaction ACS_DP_ANONYMIZATION)
  Removes user names for data that is not going to be archived.
- *Garbage Collector* (transaction ACS_DP_GCO)
  Deletes unwanted data.
- *Display Data Protection Logs* (transaction ACS_DP_LOG)
  Displays the application log for data protection activities.
- *Archive Administration* (transaction SARA)
  Archives data based on the *Archive Development Kit* (ADK).
- *Data Destruction* (transaction ILM_DESTRUCTION)
  SAP Information Lifecycle Management (ILM) can be used to delete the archived data based on retention rules on a defined point in time.
- *Read Access Logging Manager* (transaction SRALMANAGER))
  Read Access Logging is used to monitor and log read access to sensitive data. This data may be categorized as sensitive by law, by external company policy, or by internal company policy.

> i Note
>
> For more information, see the *Security Guide.*

Related Information

Removing User Names [page 105]

Garbage Collector [page 106]

Displaying the Data Protection Logs [page 108]

Data Archiving in SAP Audit Management [page 107]

12.1 Removing User Names

You can use this function to remove the user names from the system once the residence period has been reached.

To remove the user names from business objects, call transaction *Remove User Names* (ACS_DP_ANONYMIZATION) in the back-end system.

You can also run this function in test mode.

Prerequisites

You have defined the residence period for each business object in Customizing activity *Define Residence Period*.

Example

Depending on the structure of the business object, you can use this function to remove the *Created By* user names, *Last Changed By* user names, or *Executed By* user names.

> i Note
>
> For more information, see the detailed documentation in the back-end system.

12.2 Garbage Collector

You can use this function to delete unwanted data.

To delete objects that are no longer referenced or no longer needed, call transaction *Garbage Collector* (`ACS_DP_GCO`) in the back-end system

You can also run this function in test mode.

Prerequisites

You have defined the residence period for the simulated alert input data in Customizing activity *Define Residence Period*.

Results

This function deletes the following data:

- Alert input data for mass detection
- Simulated alert input data
    - Mass detection simulation results
    - Results of the calibration
    - Intermediate results of the delta address screening
- Assignments to user groups
- Personal settings

i Note

For more information, see the detailed documentation in the back-end system.

Application Log

You can display the application log for the *Garbage Collector* using transaction *Display Data Protection Logs* (ACS_DP_LOG).

Choose the log object ACS_DATAPROTECTION and the subobject DELETION.

Related Information

Displaying the Data Protection Logs [page 108]

12.3 Data Archiving in SAP Audit Management

Data archiving is used to remove mass data from the database that is no longer required in the system but must be kept in a format that can be analyzed.

The following table shows the available archiving objects and their ILM objects:

Object	Archiving Object	ILM Object
Action	AUD_ACTION	AUD_ACTION
Audit	AUD_AUDIT	AUD_AUDIT
Detection Working Paper	AUD_DETWPA	AUD_DETWPA
Document Working Paper	AUD_DOCWPA	AUD_DOCWPA
Detection Task	AUD_DTASK	AUD_DTASK
Export Job	AUD_EXJOB	AUD_EXJOB
Import Job	AUD_IMJOB	AUD_IMJOB
Manual Task	AUD_MTASK	AUD_MTASK
Audit Plan	AUD_PLAN	AUD_PLAN

Object	Archiving Object	ILM Object
Question Task	AUD_QTASK	AUD_QTASK
Zip Download Job	AUD_ZPJOB	AUD_ZPJOB

Dependencies

Before archiving, the system checks if the preconditions for archiving data are met. Then, the write program writes the data in an archive file. The delete program deletes the archived data from the database. It is still possible to display this data in the archive file.

The SAP data archiving concept is based on the Archive Development Kit (ADK) using the *Archive Administration* function (transaction SARA).

For more information, see the *Data Archiving* documentation on the SAP Help Portal at http://help.sap.com/nw.

For more information, see the *SAP Information Lifecycle Management (ILM)* documentation on the SAP Help Portal at http://help.sap.com.

12.4 Displaying the Data Protection Logs

You can use this function to display the data protection logs.

To display the application log, call transaction *Display Data Protection Logs* (ACS_DP_LOG) in the back-end system.

Selection Parameters

You can filter the logs, for example, by the following criteria:

- **Object and subobject**
  The object ACS_DATAPROTECTION (*Log for Data Protection*) is already set as the default.
  The subobjects could be the following:
  - ANONYMOUS for user names that have been removed from system administration data
  - ARCHIVING for archiving preparation

    > i Note
    >
    > To display the log for data archiving, choose the **object** ARCHIVING.

  - DELETION for data that has been deleted with the garbage collector

- External ID
  This ID was assigned by the application program. (It is a combination of the report name, time stamp, and user name.)
- Program
  Enter the name of the program that caused the logged event: `ACS_DP_GARBAGE_COLLECTOR` (*Garbage Collector*), `ACS_BO_ANONYMOUS`(*Remove User Names*), `BPCM_BO_ORG_END_BUS_REL` (*End of Business Relation for Organization*), `BPCM_BO_PERSON_END_BUS_REL` (*End of Business Relation: Person*)
- **Time restriction**, **user**, or **log class**

Results

Examples for log messages that have been created for the subobject `DELETION` are:

- *Processing simulation results*
  `<120>` records deleted
- *Processing invalid user assignments*
  `<10>` user assignments deleted from groups

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon ➦ : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon ➦: You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

www.sap.com/contactsap

THE BEST RUN SAP