Management of Internal Controls: Security Guide

ADDON.MIC_GENERAL

Release 670

Copyright

Icons in Body Text

Icon	Meaning
⚠	Caution
💬	Example
💡	Note
🧭	Recommendation
Syn	Syntax

Additional icons are used in SAP Library documentation to help you identify different types of information at a glance. For more information, see *Help on Help* → *General Information Classes and Information Classes for Business Information Warehouse* on the first page of any version of *SAP Library*.

Typographic Conventions

Type Style	Description
Example text	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation.
Example text	Emphasized words or phrases in body text, graphic titles, and table titles.
EXAMPLE TEXT	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
`Example text`	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example text`	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example text>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE TEXT`	Keys on the keyboard, for example, `F2` or `ENTER`.

Management of Internal Controls: Security Guide

Use

This Security Guide describes the aspects of the *Management of Internal Controls* (MIC) component that relate to security. MIC forms part of the software component FINBASIS and uses the application server (AS), *Process Integration (XI)*, and *Business Intelligence (BI) from SAP NetWeaver*.

Consequently, the following security guides also apply to MIC:

- SAP NetWeaver Security Guide
- SAP Web AS Security Guide ABAP
- SAP Exchange Infrastructure Security Guide
- SAP Business Information Warehouse Security Guide

You find these guides on SAP Service Marketplace at **`service.sap.com/securityguide`**.

For more information relevant to security, see SAP Service Marketplace at **`service.sap.com/security`**.

Target Audience of the Guide

- Technical consultants
- System administrators

The security guides provide information on all phases of the software life cycle.

Features

The security guide provides information on the following topics:

- **Technical System Landscape**

  This section lists the other systems with which MIC can communicate.

- **User Management and Authorizations**

  This section provides an overview of the following aspects:

  - User Management
  - Roles and Authorizations Concept Specific to MIC
  - Integration into Single Sign-On Environments

- **Communication Channel Security**

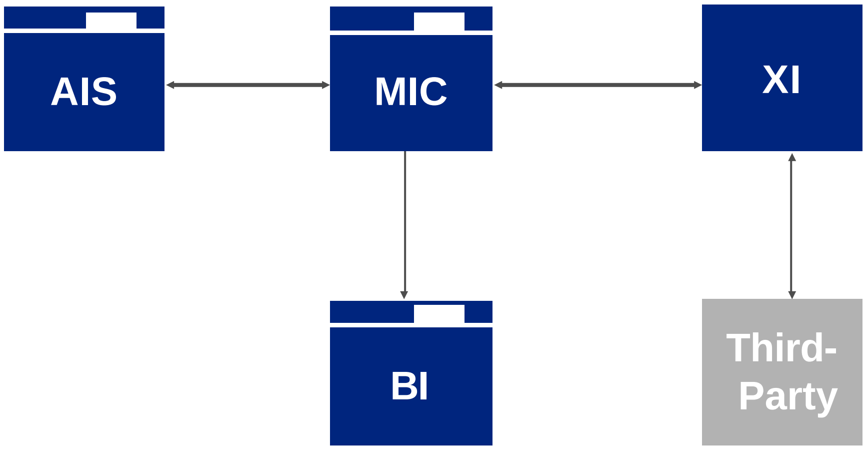
  This section provides an overview of the communication paths used by MIC and the security mechanisms that apply.

- **Data Storage Security**

  This section provides an overview of the various data storage options for MIC data.

Technical System Landscape

The following figure provides an overview of the technical system landscape of the component *Management of Internal Controls (MIC)*:



MIC can exchange data with the following systems:

- MIC users can display reports from the *Audit Information System (AIS)*, which can be run on the same system as MIC or on a different system.
- MIC data can be extracted into an *SAP NetWeaver* Business Intelligence system (BI system).
- Via the *SAP NetWeaver Process Integration (XI)*, data can be exchanged with third-party systems. You can transfer test logs from (semi-)automated tests and structure data (from the central process catalog, for example) into the MIC system.

For information about the communication paths, see Communication Channel Security [Page 31].

User Management and Authorizations

MIC uses the user management and the authorization concept delivered with the *SAP NetWeaver* platform, in particular *SAP Web Application Server ABAP*. For this reason, the security recommendations and guidelines described in the *SAP Web AS Security Guide for ABAP Technology* also apply for MIC.

In addition to these guidelines, the following sections include information about user management and the authorizations applying specifically to MIC:

- User Management [Page 8]

  This section lists the user management tools and the necessary user types.

- Roles and Authorizations Concept [Page 9]

  This section describes the MIC-specific roles and authorizations concept that is based in part on the functions of the *SAP Web Application Server ABAP* (see Standard Roles and Authorization Objects [Page 10]) and in part on the functions unique to MIC (see Editing MIC-Specific Roles [Page 12]).

- Integration with Single Sign-On Environment [Page 30]

  This topic describes how MIC supports Single Sign-On mechanisms.

User Management

Use

MIC user management uses the mechanisms provided by *SAP NetWeaver*, such as tools, user types, and the password concept. For an overview of how these mechanisms affect MIC, see the sections below. Furthermore, the system outputs a list of users that are required for operations.

User Management Tool

MIC uses user and role maintenance from *SAP Web AS ABAP* (transactions SU01, PFCG) For more information, see Users and Roles (BC-SEC-USR) [External]. To find out which roles are delivered for MIC, see under Standard Roles and Authorization Objects [Page 10].

User Types

It is often necessary to create different security policies for different types of users. For example, your policy may specify that users who perform their tasks interactively have to change their passwords on a regular basis, but not those users who perform their tasks using background processing.

Examples of user types required for MIC:

- Individual users (dialog users)
  - Required for logging on to the *SAP GUI for Windows* for configuring MIC and for MIC administration
  - Required for logging on to the *People-Centric User Interface* for the operational use of MIC
  - Required for the RFC connection to the BI system
- Technical users
  - A *system user* is required for the workflow within MIC, for example (user WF-BATCH must have authorization for authorization profile SAP_ALL)
  - A *communications user* can be required in order to set up the integration with the *Audit Information System (AIS)* for the RFC connection to the AIS system. Alternatively, you can define the RFC connection as a trusted system connection.
  - A *service user* is required for the connection of external applications using the *Exchange Infrastructure (XI)*. The user must have the corresponding XI authorization as well as the authorization for the standard role *Management of Internal Controls – Business User (SAP_CGV_MIC_BUSINESS_USER).* For more information, see the *SAP Exchange Infrastructure Security Guide* under *Service Users for Message Exchange*.

Roles and Authorizations Concept

Use

For *Management of Internal Controls (MIC)*, a large number of employees need to perform tasks in a variety of functions. Consequently, a special roles and authorizations concept has been created for this purpose. Besides the general SAP standard roles that are edited by the system administrator in transaction PFCG, there are also MIC-specific roles comprising a variety of delivered tasks. These MIC-specific roles and their respective tasks allow you to manage the detailed authorizations and the workflow between those involved.

Features

For information about the general **standard roles** delivered with MIC, see Standard Roles and Authorization Objects [Page 10].

The **MIC-specific roles** refine the authorizations delivered in the standard role *Management of Internal Controls - Business User (SAP_CGV_MIC_BUSINESS_USER)*. An MIC-specific role consists of different tasks with authorizations attached. You can specify which tasks belong to which role. For more information, see Editing MIC-Specific Roles [Page 12].

The assignment of an MIC-specific role to one or more persons is dependent on an object (for example, an organizational unit). The assignment is performed in a Web application by different persons throughout the organization hierarchy. The power user triggers this process for the highest level of the organization hierarchy. For more information, see Assigning Roles to Persons [Page 29].

To ensure the **segregation of duties** so that the same person is not authorized to perform an assessment as well as the validation of that assessment, for example, you can define conflict groups. You include in a conflict group any tasks that must not be performed by the same person. You can use these conflict groups to run a check to establish whether the defined segregation of duties is actually reflected in the system.

Activities

1. The system administrator copies the delivered standard role *Management of Internal Controls – All Authorizations (SAP_CGV_MIC_ALL)*, makes any necessary adjustments, and assigns the adjusted copy of the standard role to the MIC power user.
2. The power user edits the MIC-specific roles.
3. The power user defines conflict groups.
4. The power user starts the role assignment procedure in the navigational area on the start page.
5. The power user checks whether the segregation of duties defined in the conflict groups is enforced by the system.

Standard Roles and Authorization Objects

Use

The authorization concept of the *SAP NetWeaver Application Server* uses the assignment of authorizations to users on the basis of roles. Some general SAP standard roles are delivered with MIC. You can copy and adjust them in Customizing under *SAP NetWeaver* → *Application Server* → *System Administration* → *Users and Authorizations* → *Maintain Authorizations and Profiles Using Profile Generator* → *Maintain Roles* (transaction PFCG).

Integration

The standard roles are refined using the MIC-specific Roles and Authorization Concept [Page 9].

Features

Standard Roles

MIC uses the following standard roles:

- *Management of Internal Controls - Customizing (SAP_CGV_MIC_CUSTOMIZING)*

  This role contains all necessary authorizations to make the Customizing settings for MIC. This role does not contain any authorizations for the Web applications.

- *Management of Internal Controls - Business User (SAP_CGV_MIC_BUSINESS_USER)*

  A user with this role is only authorized to perform those specific tasks prescribed by the detailed role concept for MIC. All users that have this role assigned to them must also have at least one MIC-specific role assigned to them. A user may use the Web applications that are specified by the tasks in the MIC-specific role.

- *Management of Internal Controls - Power User (SAP_CGV_MIC_ALL)*

  When this role is assigned to a user, that user is made a power user. In addition to the authorizations that the business user has, a power user also has authorization for administration functions in the MIC Implementation Guide, such as the expert mode for structure setup [External]. Moreover, the user has special authorizations in the People-Centric UI, such as those for editing roles and for starting role assignment to persons (see Assigning Roles to Persons [Page 29]).

- *Management of Internal Controls - Display (SAP_CGV_MIC_DISPLAY)*

  A user with this role can display Customizing for MIC in the SAP GUI. This role is useful for external auditors, for example. We recommend using this role in addition to the business user role.

For more information, see the documentation on the individual roles in transaction PFCG.

Standard Authorization Objects Relevant to Security

Authorizations for objects of applications belonging to the *Application Server* and used in MIC are relevant to security in MIC. If you run MIC in a system in which the applications used by MIC are also used productively in other projects, then you need to ensure that you manage the authorizations for the MIC-specific objects separately from the other objects.

- Authorization object *Personnel Planning (PLOG)* from Organizational Management

  The general object types *Organizational Unit* und *Person* are used in MIC together with other MIC-specific object types.

Note, therefore, that the organizational units and persons created in other projects are also available in MIC (and vice versa).

- Various authorization objects in *Case Management* and *Records Management*

  Assessments, *tests*, *issues*, and *remediation plans* are stored in Case or Records Management. The RMS ID *FOPC_SOA* is relevant for MIC.

Activities

1. Copy the general SAP roles delivered with MIC, and adjust the authorizations in these roles to suit the circumstances in your system.
2. Assign the roles you have adjusted to the appropriate users. While doing so, ensure that **no** user has been assigned role *Management of Internal Controls – All Authorizations (SAP_CGV_MIC_ALL)* as well as role *Management of Internal Controls - Business User (SAP_CGV_MIC_BUSINESS_USER)*.

Editing MIC-Specific Roles

Use

An MIC power user can adjust the MIC-specific roles that are delivered in BC Sets and in this way specify the authorizations of a role by assigning the individual tasks.

Features

The power user has the following options for editing MIC-specific roles:

- In Customizing for MIC under *Edit Roles*
- Using a Web application that can be called up from the MIC start page

SAP delivers sample roles in a BC Set. To be able to use these sample roles, you need to activate the BC Set in Customizing. All other activities for editing roles are possible both in Customizing and in the Web application, although the user interface in the Web application is easier to use.

When editing a role, you assign all the tasks to it that anybody assigned to that role should be allowed to perform. You also specify the role level.

The **role level** defines whether the tasks can be performed for the entire corporate group, for a single organizational unit, for a process group, for a process, or for a process step.

The **tasks** are delivered by SAP and cannot be changed. Each task has the following attributes:

- *Minimum Role Level*: The only tasks you can assign to a role are those with a minimum role level corresponding to the level entered for the role. For example, you can only assign the task *Perform Sign-Off at Corporate Level* (for which the minimum role level = group) to a role with *Corporate* level.
- *Restricted to One Role*: Tasks for which this indicator is selected can only be assigned to one role. Furthermore, the following restriction applies to role assignment: When a role contains a task flagged with this indicator, that role may only be assigned to **just one person for an object**.
- *Processing by One Work Item Recipient Suffices*: Tasks flagged with this indicator can be performed by more than one user. However, it is sufficient if only one user performs the task. As soon as one user has completed the task, it is then completed for all other users to whom the task is assigned.
- *Web application that the task calls up*: Different tasks can call up the same Web application. For example, the task *Assign Process to Organizational Unit* and the task *Edit Attributes of Process Groups Specific to Org Units* both call up the Web application *Process Assignment for Org Unit*. If a person only has authorization for one of the tasks, then that person may only perform that task in the corresponding Web application. If, however, a person has authorization for both tasks, then he/she may perform both, regardless of the task from which the Web application was called up. In this latter case, it is sufficient for just one of the tasks to be scheduled. In this way, you can restrict the number of tasks that need to be sent.

For an overview of the delivered tasks and their attributes, see the following sections:

- Tasks: Central Structure Setup [Page 14]
- Tasks: Structure Setup Specific to Organizational Units [Page 16]
- Tasks: Control Assessments and Tests [Page 21]
- Tasks: Management Control Assessment and Test [Page 24]
- Tasks: Reporting and Sign-Off [Page 27]

The task *Create User* is handled differently because a special authorization is required for this task. For more information, see Creating Users and Connecting Users to Persons [External].

Analyses

To find out which roles contain a task, you can search for a task in the Web application for processing roles. In this way, you can display all roles that the task is assigned to. Moreover, you can use Authorization Analysis [External].

Activities

1. If you want to use the delivered sample roles, activate the relevant BC Set in Customizing. For information about the procedure for this, see the documentation on the IMG activity *Edit Roles.*
2. Change the delivered sample roles or create your own roles.
3. Activate the roles that you would like to use and then save your entries.

Tasks: Central Structure Setup

Task Group: ***Central Structure Setup***

Task	Description	Role Level	Restricted to One Role	Processing by One Work Item Recipient Suffices	Web Application Called
Display Role (DISP-ROLE)	Display all roles created and all tasks assigned by power user (see Roles and Authorizations Concept [Page 9])	Process Step			Edit Roles
Edit Organizational Hierarchy (EDIT-HIER)	Create/change organizational hierarchy [External], insert new nodes, and so forth	Corporate	X		Organizational Hierarchy
Display Organizational Hierarchy (DISP-HIER)	Display entire organizational hierarchy and detailed information on organizational units	Process Step			Organizational Hierarchy
Document Organizational Units in Scope (PERF-SCOPO)	Define reasoning for decision to include organizational units in project scope [External] (or to exclude them from project scope)	Corporate	X		Organizational Units in Scope
Display Organizational Units in Scope (DISP-SCOPO)	Display reasoning behind decisions relating to the project scope	Process Step			Organizational Units in Scope
Edit Central Process Catalog (EDIT-CPCAT)	Create/change hierarchy and attributes for process groups and processes, create/change central process steps, define P-CO-R assignment, assign account groups (see Central Process Catalog [External])	Corporate	X		Central Process Catalog
Display Central Process Catalog (DISP-CPCAT)	Display entire central process catalog	Process Step			Central Process Catalog
Edit General Control Attributes in Central Process Catalog (EDIT-CCATR)	When central process step has been defined as a control, define all attributes and assignments for the control centrally (see Documenting Controls Centrally [External])	Corporate			Documentation of Controls

Edit Account Group Hierarchy (EDIT-ACCH)	Create/change hierarchy and attributes of account groups (see Account Group Hierarchy [External])	Corporate	X		Account Group Hierarchy
Display Account Group Hierarchy (DISP-ACCH)	Display entire account group hierarchy	Process Step			Account Group Hierarchy
Edit Management Control Catalog (EDIT-MCCAT)	Create/change hierarchy of management control groups and management controls, define central descriptions (see Management Control Catalog [External])	Corporate	X		Management Control Catalog
Edit Description of Assessment of a Management Control (EDIT-MCASD)	Create central description in catalog of how a management control should be assessed	Corporate	X		Management Control Catalog
Edit Description of a Test of a Management Control (EDIT-MCTED)	Create central description in catalog of how a management control should be tested	Corporate	X		Management Control Catalog
Display Management Control Catalog (DISP-MCCAT)	Display entire management control catalog	Process Step			Management Control Catalog
Edit Central Settings for Scheduling (EDIT-CSCH)	Specify centrally how often and when specific tasks are to be performed (see Task Scheduling [External])	Corporate			Central Scheduling of Tasks
Display Central Settings for Scheduling (DISP-CSCH)	Display central settings for task scheduling	Process Step			Central Scheduling of Tasks
Assign Delegates Centrally (ASGN-DELC)	Enter delegates [External] for oneself and other persons	Corporate	X		Central Assignment of Delegates
Assign Own Delegates (ASGN-DELO)	Only enter delegates for oneself	Process Step			Assignment of Own Delegates

Tasks: Structure Setup Specific to Organizational Units

Task Group: ***Structure Setup Dependent on Org Unit***

Task	Description	Role Level	Restricted to One Role	Processing by One Work Item Recipient Suffices	Web Application Called
Assign Roles for Corporate and Next Level Down (ASGN-RLCOR)	Assign roles to persons at the corporate level and for the subordinate organizational units directly beneath it (see Assigning Roles to Persons [Page 29])	Corporate	X		Role Assignment
Assign Replacement at Corporate Level (ASGN-REPLC)	Assign replacements at corporate level (see Replacement [External])	Corporate			Assignment of Replacements
Assign Roles for Given Organizational Unit and Next Level Down (ASGN-RLORG)	Assign roles to persons for an organizational unit and for the subordinate organizational units directly beneath it	Org Unit	X		Role Assignment
Assign Replacement at Org Unit Level (ASGN-REPLO)	Assign replacements for the organizational unit and subordinate objects	Org Unit			Assignment of Replacements
Assign Roles for Top Process Group in Given Organizational Unit (ASGN-RLOPG)	Assign roles to persons for the top process groups of an organizational unit	Org Unit	X		Role Assignment
Assign Roles for Given Process Group and Next Level Down (ASGN-RLPGR)	Assign roles to persons for a process group and for the subordinate process groups and processes directly beneath it	Process Group	X		Role Assignment
Assign Roles for Process and Subordinate Controls (ASGN-RLPRC)	Assign roles to persons for a process and for the process steps defined as a control in the process	Process	X		Role Assignment
Assign Roles for Control (ASGN-RLCNT)	Assign roles to persons for a process step defined as a control	Process Step			Documentation of Controls

Create User (CREA-USRID)	Have a user ID created by the system administrator and connect this user ID to the person (see Creating Users and Connecting Users to Persons [External])	Org Unit		X	Only possible in SAP GUI
Specify Significance of Accounts for Organizational Unit (EDIT-ACCSO)	Specify for an organizational unit which account groups are significant (see Significance of Account Groups for Organizational Unit [External]).	Org Unit	X		Processes and Account Groups for the Organizational Unit
Display Significance of Accounts for Organizational Unit (DISP-ACCSO)	Display significance of account groups for an organizational unit	Process Step			Processes and Account Groups for the Organizational Unit
Perform Scoping of Processes (PERF-SCOPP)	Specify for an organizational unit which processes fall within the project scope and document why (see Processes in Scope [External])	Org Unit	X		Processes in Scope
Display Processes in Scope (DISP-SCOPP)	Display processes that fall within the project scope for an organizational unit	Process Step			Processes in Scope
Assign Process to Organizational Unit (ASGN-PRORG)	Accept for organizational unit processes falling in project scope; edit process attributes specific to organizational unit (see Accepting Processes and Documenting Controls [External])	Org Unit	X		Processes and Account Groups for the Organizational Unit
Display Process Group Attributes Specific to Org Units (DISP-OUPGA)	Display process group attributes specific to organizational units (such as necessity of validation)	Process Step			Processes and Account Groups for the Organizational Unit
Edit Process Group Attributes Specific to Org Units (EDIT-OUPGA)	Edit process group attributes specific to org units	Process Group			Processes and Account Groups for the Organizational Unit
Display Process Attributes Specific to	Display process attributes specific to	Process Step			Processes and Account Groups

Org Units (DISP-OUPRA)	organizational units (such as necessity of validation)				for the Organizational Unit
Edit Process Attributes Specific to Org Units (EDIT-OUPRA)	Edit process attributes specific to org units	Process			Processes and Account Groups for the Organizational Unit
Edit Documentation on Process Change (EDIT-OUPRC)	Documenting Process Changes [External]	Process			Processes and Account Groups for the Organizational Unit
Edit Process Steps Specific to Org Units (EDIT-OUPRS)	Edit copied process steps, create/change local process steps, edit process step attributes	Process			Processes and Account Groups for the Organizational Unit
Edit General Control Attributes (EDIT-GENCA)	Edit the general control attributes for local or copied process steps defined as controls (excluding assessment and test attributes)	Process Step	X		Documentation of Controls
Assign Control to Process - Control Objective - Risk (P-CO-R) (ASGN-CPCOR)	Assign control to the P-CO-R structure defined in the process catalog and select control type	Process Step			Documentation of Controls
Assign Referenced Control to Process - Control Objective - Risk (P-CO-R) (ASGN-CRCOR)	Assign control of a different process to the P-CO-R structure defined in the process catalog and select control type	Process	X		Processes and Account Groups for the Organizational Unit
Assign Controls to Financial Statement Assertions (ASGN-ASS2C)	Assign control to control groups and their FS assertions	Process Step	X		Documentation of Controls
General Control Attributes: Edit Assessment Attributes (EDIT-GCAMT)	Of the general control attributes, only edit the control assessment attributes (such as control maturity target)	Process Step	X		Documentation of Controls
General Control Attributes: Edit Test Attributes (EDIT-GCATA)	Of the general control attributes, only edit the control test attributes (such as testing technique)	Process Step	X		Documentation of Controls
General Control Attributes: Edit AIS Reports (EDIT-	Under the general control attributes, assign the reports of	Process Step			Documentation of Controls

COAIS)	the *Audit Information System*				
Display Process Hierarchies of all Organizational Units (DISP-PRHIE)	Display process groups, processes, and process steps for all organizational units	Process Step			Central Process Catalog
Display General Control Attributes (DISP-GENCA)	Display all general attributes and assignments for the control	Process Step			Documentation of Controls
Assign Management Controls to Organizational Units (ASGN-MC2OU)	Accept centrally-defined management controls for organizational unit, create local description (see Accepting Management Controls [External]).	Org Unit	X		Assignment of Management Controls
Assign Management Controls to Process Group (ASGN-MC2PG)	Accept centrally-defined management controls for process group, create local description of the control	Process Group	X		Assignment of Management Controls
Edit Local Description of Assessment of a Mgmt Control for Organizational Unit (EDIT-MADOU)	Create description of how the management control should be assessed specific to organizational unit	Org Unit	X		Assignment of Management Controls
Edit Local Description of Test of a Mgmt Control for Organizational Unit (EDIT-MTDOU)	Create description of how the management control should be tested specific to organizational unit	Org Unit	X		Assignment of Management Controls
Edit Local Description of Assessment of a Mgmt Control for Process Group (EDIT-MADPG)	Create description of how the management control should be assessed specific to process group	Process Group	X		Assignment of Management Controls
Edit Local Description of Test of a Mgmt Control for Process Group (EDIT-MTDPG)	Create description of how the management control should be tested specific to process group	Process Group	X		Assignment of Management Controls
Edit "To Be Tested" Attribute of a Management Control for Organizational Unit (EDIT-MTAOU)	Specify for organizational unit whether a management control should be tested	Org Unit	X		Assignment of Management Controls
Edit "To Be Tested" Attribute of a Management Control for Process Group	Specify for process group whether a management control should be tested	Process Group	X		Assignment of Management Controls

(EDIT-MTAPG)					
Edit Scheduling Settings for Organizational Unit (EDIT-OUSCH)	Change central settings governing Task Scheduling [External] for organizational unit	Org Unit	X		Scheduling Task for Organizational Unit
Display Scheduling Settings for Organizational Unit (DISP-OUSCH)	Display task scheduling settings changed for an organizational unit	Process Step			Scheduling Task for Organizational Unit

Tasks: Control Assessments and Tests

Task Group *Assessment of Control Design and Efficiency*

Task	**Description**	**Role Level**	**Restricted to One Role**	**Processing by One Work Item Recipient Suffices**	**Web Application Called**
Perform Control Design Assessment (PERF-CDASS)	Enter result of control design assessment in system, reporting issues where necessary (see Assessment of Control Design and Efficiency [External])	Process Step	X		Control Design Assessment
Display Control Design Assessment (DISP-CDASS)	Display result of control design assessment	Process Step			Control Design Assessment
Validate Control Design Assessment (VALI-CDASS)	When validation activated, check result of control design assessment and confirm or send back	Process		X	Control Design Assessment
Perform Control Efficiency Assessment (PERF-CEASS)	Enter result of control efficiency assessment, reporting issues where necessary	Process Step	X		Control Efficiency Assessment
Display Control Efficiency Assessment (DISP-CEASS)	Display result of control efficiency assessment	Process Step			Control Efficiency Assessment
Validate Control Efficiency Assessment (VALI-CEASS)	When validation activated, check result of control efficiency assessment and confirm or send back	Process		X	Control Efficiency Assessment

Task Group *Process Design Assessment*

Task	Description	Role Level	Restricted to One Role	Processing by One Work Item Recipient Suffices	Web Application Called
Perform Process Design Assessment (PERF-PDASS)	Enter result of process design assessment in system, reporting issues where necessary (see Process Design Assessment [External])	Process	X		Process Design Assessment
Display Process Design Assessment (DISP-PDASS)	Display result of process design assessment	Process			Process Design Assessment
Validate Process Design Assessment (VALI-PDASS)	When validation activated, check result of process design assessment and confirm or send back	Process Group		X	Process Design Assessment

Task Group *Test Effectiveness of a Control*

Task	Description	Role Level	Restricted to One Role	Processing by One Work Item Recipient Suffices	Web Application Called
Mass Assignment of Testers to Controls (ASGN-MT2CN)	Assign testers centrally for all controls of an org unit or process group	Process Group			Mass Tester Assignment Controls/Management Controls
Assign Tester (ASGN-TSTER)	Assign persons for testing control effectiveness (see Test of Control Effectiveness [External])	Process	X		Tester Assignment
Display Notification (DISP-NOTE)	Notifications from an external system (using	**No** role level because task cannot be			Notifications

	XI interface) in which (semi-)automated tests are performed	assigned to any role			
Test Control Effectiveness (PERF-TEST)	Test control effectiveness; may be performed by all persons who were assigned as testers	**No** role level because task cannot be assigned to any role			Testing Control Effectiveness
Display Test Results (DISP-TSTRE)	Display test logs for effectiveness test of a control	Process Step			Testing Control Effectiveness
Receive Issues from Effectiveness Test (RECE-EFISO)	Predefined processor of issues reported during control effectiveness test; can be overwritten by person who reported issue	Process	X		

Tasks: Management Control Assessment and Test

Task Group *Assessment and Test of Management Controls*

Task	Description	Role Level	Restricted to One Role	Processing by One Work Item Recipient Suffices	Web Application Called
Mass Assignment of Testers to Management Controls (ASGN-MT2MC)	Assign testers centrally for all management controls of an org unit or process group	Process Group			Mass Tester Assignment Controls/Mgmt Controls
Assign Testers for Management Controls (Org Unit) (ASGN-MCTOU)	Assign persons for testing management controls for organizational unit	Org Unit	X		Tester Assignment
Assign Testers for Management Controls (Process Group) (ASGN-MCTPG)	Assign persons for testing management controls for process group	Process Group	X		Tester Assignment
Perform Management Control Assessment at Org Unit Level (PERF-MCAOU)	Enter result of management control assessment for org unit in system, reporting issues where necessary (see Management Control Assessment and Test [External])	Org Unit	X		Management Control Assessment
Display Management Control Assessment at Org Unit Level (DISP-MCAOU)	Display result of management control assessment for organizational unit	Org Unit			Management Control Assessment
Perform Management Control Assessment at Process Group Level (PERF-MCAPG)	Enter result of management control assessment for process group in system, report issues where necessary	Process Group	X		Management Control Assessment
Display Management Control Assessment at	Display result of management control assessment for	Process Group			Management Control Assessment

Process Group Level (DISP-MCAPG)	process group				
Validate Management Control Assessment for Top Organizational Unit (VALI-MCACP)	When validation activated, check result of management control assessment for top node of organizational hierarchy and confirm or send back	Corporate		X	Management Control Assessment
Validate Management Control Assessment for Subordinate Organizational Unit (VALI-MCAOU)	When validation activated, check result of management control assessment for subordinate organizational units and confirm or send back	Org Unit		X	Management Control Assessment
Validate Management Control Assessment for Top Process Group (VALI-MCTPG)	When validation activated, check result of management control assessment for top process group of organizational unit and confirm or send back	Org Unit		X	Management Control Assessment
Validate Management Control Assessment for Subordinate Process Group (VALI-MCAPG)	When validation activated, check result of management control assessment for subordinate process groups and confirm or send back	Process Group		X	Management Control Assessment
Perform Management Controls Test at Org Unit Level (PERF-MCTOU)	Create test log after management controls test for organizational unit; may be performed by persons who were assigned as testers	**No** role level because task cannot be assigned to any role			Management Controls Test
Display Management Controls Test at Org Unit Level	Display result of management controls test for	Org Unit			Management Controls Test

(DISP-MCTOU)	organizational unit				
Perform Management Controls Test at Process Group Level (PERF-MCTPG)	Create test log after management controls test for process group; may be performed by persons who were assigned as testers	**No** role level because task cannot be assigned to any role			Management Controls Test
Display Management Controls Test at Process Group Level (DISP-MCTPG)	Display result of management controls test for process group	Process Group			Management Controls Test
Receive Issues from Management Controls Test at Org Unit Level (RECE-MCISO)	Predefined processor of issues reported during management controls test; can be overwritten by person who reported issue	Org Unit	X		
Receive Issues from Management Controls Test at Process Group Level (RECE-MCISP)	Predefined processor of issues reported during management controls test; can be overwritten by person who reported issue	Process Group	X		

Tasks: Reporting and Sign-Off

Task Group *Reporting*

Task	Description	Role Level	Restricted to One Role	Processing by One Work Item Recipient Suffices	Web Application Called
Display Hierarchical Reports (DISP-ANALY)	Display data for the area of responsibility in hierarchical reports in Reporting [External]	Process			Reporting
Display Tabular Reports (DISP-FLATR)	Display data for the area of responsibility in tabular reports	Process			Reporting
Display Management Reports (DISP-MNGRE)	Display aggregated data for the area of responsibility in management reports	Process			Reporting
Print Report (PERF-PRINT)	Create and print Print Reports [External]	Process Step			Print Reports
Display Change Analysis (DISP-CHGAN)	Display changes to data over different timeframes (see Change Analysis [External])	Org Unit			Change Analysis
Display Authorization Analysis (DISP-SCREP)	Display assignments in the roles and authorizations concept (see Authorization Analysis [External])	Process			Authorization Analysis

Task Group *Sign-Off*

Task	Description	Role Level	Restricted to One Role	Processing by One Work Item Recipient Suffices	Web Application Called
Perform Sign-Off (PERF-SOFOU)	Perform sign-off [External] for an organizational unit and, once sign-off has been performed for all organizational units,	Org Unit	X		Sign-Off

	perform corporate sign-off				
Display Sign-Off (DISP-SIGNO)	Display sign-off for organizational units in area of responsibility	Org Unit			Sign-Off

Assigning Roles to Persons

Purpose

When you assign a person to a role in combination with an object (such as an organizational unit), that person receives the authorization to perform the tasks belonging to that role for that object.

You assign roles to persons in one of the Web applications that can be accessed from the start page [External]. Role assignment takes place using the domino principle throughout the organizational hierarchy and the assigned processes.

Prerequisites

- The roles have been created and activated (see Roles and Authorizations Concept [Page 9]).
- The organizational hierarchy [External] has been defined.

Process Flow

1. The power user automatically has authorization for the task *Start Role Assignment Procedure*. He or she starts the assignment procedure by choosing *Role Assignment* in the navigation area of the start page [External]. The power user then assigns a person (or a user, if one has already been created) to the role containing the task *Assign Roles for Corporate and Next Level Down (ASGN-RLCOR)*.
   - If the person entered does not yet exist in the system, the system issues a message, and an additional area appears in the middle of the screen. To create the person, choose *Create Person*.
   - If a person does not yet exist for the user entered in the system, a person is created automatically.
2. The power user assigns a role with the task *Create User (CREA-USRID)* to a user that has already been created.
3. If the power user has assigned a person in the first step as opposed to a user, a user must be created for that person. For more information, see Creating Users and Connecting Users to Persons [External].
4. The person who now has authorization for the task *Assign Roles for Corporate and Next Level Down* receives this task in their task list on the start page.
5. This person assigns persons or users to the role containing the task *Assign Roles for Given Organizational Unit and Next Level Down (ASGN-RLORG)*. This step is performed for all organizational units occurring directly beneath the corporate group level in the organizational hierarchy.
6. If persons instead of users are assigned, users must be created for these persons (see Creating Users and Connecting Users to Persons [External]).
7. The persons who now have authorization for the task *Assign Roles for Given Organizational Unit and Next Level Down* receive this task in their task list on the start page. Subordinate organizational units or process groups can be on the next level down. For process groups to be available, processes need to have been adopted [External] at the org unit level in the meantime.
8. Subsequent role assignments follow the same principle all the way down the organizational hierarchy and across the assigned process groups, processes, process steps, and controls.

Integration with Single Sign-On Environments

Use

MIC supports the Single Sign-On (SSO) mechanisms provided by the *SAP Web Application Server ABAP*. Consequently, the security recommendations and guidelines for user management and authentication described in the *SAP Web Application Server Security Guide* also apply to MIC.

The mechanisms supported are listed below.

Secure Network Communications (SNC)

SNC is available for user authentication and provides an SSO environment when the *SAP GUI for Windows* or *Remote Function Calls* (RFC) are used.

For more information, see *Secure Network Communications (SNC)* in the security guide of the *SAP Web Application Server*.

SAP Logon Tickets

MIC supports the use of logon tickets for SSO when the Web browser is used as the front end client. In this case, users can be issued a logon ticket after they have authenticated themselves in the original SAP system. The ticket can then be submitted to other systems (SAP or external systems) as an authentication token. The user does not need to enter a user ID or password for authentication but can access the system directly once the system has checked the logon ticket.

For more information, see *SAP Logon Tickets* in the *SAP Web Application Server* security guide.

Client Certificates

As an alternative to user authentication using a user ID and passwords, users using a Web browser as a front end client can also provide X.509 client certificates to use for authentication. In this case, user authentication is performed on the Web server using the Secure Sockets Layer protocol (SSL protocol), and no passwords need to be transferred. User authorizations apply in accordance with the authorization concept in the SAP system.

For more information, see *Client Certificates* in the security guide of the *SAP Web Application Server*.

Communication Channel Security

Use

The following table contains the communication paths used by *MIC,* the protocol used for the connection, and the type of data transferred.

Communication paths

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front end client using *SAP GUI for Windows* to application server	DIAG	All application data	Passwords
Front end client using a Web browser to application server	HTTP/HTTPS	All application data	Passwords
Audit Information System (AIS) to application server	RFC for setting up AIS integration HTTP for displaying the AIS reports	AIS reports	
External application via XI interface to application server	External application – XI: Various protocols possible (SAP standard) XI – application server: RFC	Structure data (such as central process catalog) Test logs	
Application server to BI system	RFC	All application data	

DIAG and RFC connections can be protected using Secure Network Communications (SNC). HTTPS connections are protected using the *Secure Sockets Layer* (SSL) protocol. For more information, see *Transport Layer Security* in the *SAP NetWeaver Security Guide*.

For logon to the front end client (Web browser), Single Sign-On (SSO2) must be activated **on the server side**. For more information, see SAP Note 517860.

Navigation information is communicated between the start page and the Web applications via the URL.

Data Storage Security

Use

Master data and transaction data is stored in the database of the SAP system on which MIC has been installed. Data storage occurs for the most part in *Organizational Management*, in *Case Management*, and in separate tables for this purpose. Due to the use of Organizational Management in particular, we recommend running MIC on a separate client. For more information and recommendations on the use of clients, see the application documentation under Management of Internal Controls (FIN-CGV-MIC) [External].

MIC requires a **Web browser** as the user interface. For data storage in the front end, non-persistent session cookies are used.

In some Web applications, MIC users can upload **documents** into the system. *Knowledge Provider (KPro)* is used for storing the data. Once uploaded, the documents can be accessed using an URL. The MIC-specific Roles and Authorizations Concept [Page 9] governs authorization for accessing the URL directly in the Web application. To prevent unauthorized access to the document through copying and sending the URL, an URL is only valid for a given user and for a restricted amount of time (two hours).