



Important/interesting new IAG features released in 2024 and 2025

July 17, 2025

PUBLIC



Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP's intentional or gross negligence.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

Speaker

Prashanth Kumar Duvva
Senior SAP Security and GRC Consultant, SAP

PUBLIC

Agenda



SAP GRC and Security Solutions

**What is IAG and Primary capabilities
for managing access governance**

**Important/interesting new IAG features
released in 2024 and 2025**

References

SAP GRC and Security Solutions



**Enterprise risk
and compliance**



**Identity and access
governance**



**Cybersecurity, data
protection, and privacy**



**International trade
management**

SAP Risk Management

SAP Access Control

SAP Enterprise Threat Detection

SAP Watch List Screening

SAP Process Control

**SAP Cloud Identity Access
Governance**

SAP Privacy Governance

SAP Global Trade Services

**SAP Risk and Assurance
Management**

SAP Identity Management

SAP Data Custodian

SAP Business Integrity Screening

SAP Single Sign-On

SAP Audit Management

**SAP Secure Login Service for
SAP GUI**

What is IAG and Primary capabilities for managing access governance



Important/interesting new IAG features released in 2024 and 2025

Integrations

SAP Cloud Identity Services

Identity Authentication

Authentication

Identity federation

Identity Provisioning

Identity lifecycle management

Manage groups & roles

Identity Directory

Central user store

SCIM APIs

Authorization Management

Authorization service

Policies

Syncing User Groups from Local Identity Directory Service (IdDs)

The new Identity Directory SCIM REST API allows you to manage users, groups, and custom schemas in the cloud. So, to support the IAS V2 API, the User Group sync job has been enhanced.

Applications to which your subaccount is currently subscribed



Application	Plan	Changed On	Status	
Audit Log Viewer Service	free	6 Aug 2024	Subscribed	<div><div></div><div></div></div>

Auditlog Viewer 1.0

Filter

Select categories

Jul 16, 2025, 6:42:29 PM

Jul 17, 2025, 12:42:29 AM

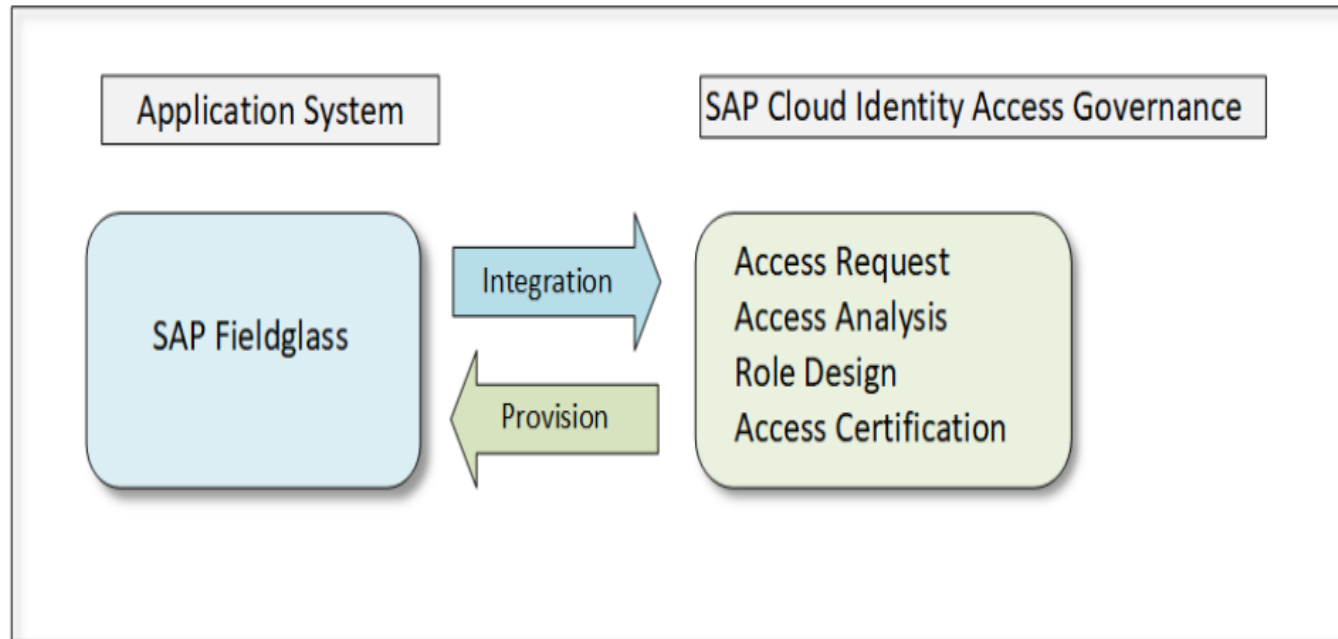
User	Time	Message	Category
No data			

Integration of SAP Cloud Identity Access Governance Audit Log Service with SAP Audit Log Service

SAP Cloud Identity Access Governance can now send relevant information for security and configuration events to SAP Audit Log Service.

Integration scenario with SAP Fieldglass

You can now assign multiple roles in SAP Fieldglass.



Additional user attribute provisioning for Ariba v2

IG now offers enhanced application support for additional user attribute provisioning to Ariba. This is available for both standalone and bridge scenarios.

The screenshot displays the SAP Cloud Identity Services interface. On the left, the 'User Management' section shows a list of users. The main area displays the details for 'ARB User22'. The 'Extensions' tab is selected, showing a 'purchasingGroup' attribute with a value of '100'. The 'Accounting' tab is also visible, showing various organizational and accounting information for the user.

User Management

First Name	Last Name	Email
ARB	User22	arb.user22@sapt-est.com
ARB	USER33	arb.user33@sapt-est.com

ARB User22

8be4e3cb-0e5c-4825-8279-4fae04367710

Details Extensions Legal Authentication Groups

companyCodeId:
controllingArea:
displayName:

purchasingGroup:
primary: true
description:
old:
displayId: 100

View Details of "ARB USER22"

General PCards Ship To Addresses Billing Addresses Accounting

View or edit the organizational and accounting information for this user.

Release Authority: (no value)

Company Code: 1000 (IDES AG)
Purch Org: 3000 (IDES USA)
Purch Group: Corporate Purchsing
GL Account: 0000200000 (Loss on disposal/sale of fixed assets)
Cost Center: 0000001000 (Corporate Services)

Scheduling Jobs

General Settings

Job Name: *

Job Category: *

▼

Send Notification:

- Access Control - Risk Definition Synchronization
- Access Control - Mitigation Control Transfer
- Privileged Access Log Synchronization
- Data Deletion
- Access Control - User Mapping Synchronization
- Access Control - Business Role Synchronization

Jobs (14)

Job Name	Job Category	Schedule Type
Log3	Privileged Access Log Synchronization	Immediate
Logsync2	Privileged Access Log Synchronization	Immediate
Logsync	Privileged Access Log Synchronization	Immediate
RISK_SYNC_01	Access Control - Risk Definition Synchronization	Immediate
RISK_SYNC	Access Control - Risk Definition Synchronization	Immediate
MC_SYNC_01	Access Control - Mitigation Control Transfer	Immediate
MC_SYNC	Access Control - Mitigation Control Transfer	Immediate

Manage Jobs

With this new app you can now schedule jobs that synchronize the data between SAP Access Control and SAP Cloud Identity Access Governance.

You can now view the last run status of jobs. Additionally, a new UI element has been introduced; the visual indicator shows errors or warnings for recent job runs.

Furthermore, introduced a new job called Privileged Access Log Synchronization under manage jobs for PAM log and review sync.

Deprovision Expired Business Role Assignments

Administrators can now remove expired Business role assignments by scheduling Deprovision Expired Business Role Assignments job via the Job Scheduler app.

Job Name: *

Job Category: * Deprovision Expired Business Role Assignments

Recurring Job: *

Start Immediately: *

- Access Analysis
- Access Control - Mitigation Control Transfer
- Access Control - Risk Definition Sync
- Access Control - User Mapping Sync Job
- Access Control Business Role Sync
- Authorization Object Sync for SAP ERP and S4HANA On-Premise
- Control Monitoring
- Deprovision Expired Business Role Assignments**
- HR Triggers
- Privileged Access Log Sync Job
- Privileged Access Review Request

Application Specific Features

<

SAP

Access Request Status ▾

🗨️

?

PKD

My Requests (1)

Search using Request ...

Q

Y

REFRESH

Request #:

Created For: ()

0

0

Days Ago

Inactive

Details

Request #: ?

Priority: ?

Created By: null (null)

Status: inactive ?

Updated: null Days Ago

Created For: null (null)

Access Requested

Additional Details

User Details

Attachments >

▼

Access

Access	Approver	Provision...	Stage	Last Upd...	Status
No Data					

Additional Details

+

Cancel Request

Help Topics

Search Help Topics

What's this App?

Request

Priority

Created by

Status

Created for

Access Requested

Access

Approver

Provisioning Action

Stage

Last updated

×

🗨️

»

SAP Companion


You can now access web-based context-sensitive in-app help for Access Analysis, Access Certification, Privileged Access Management, and Access request.

PUBLIC

Filter-Based on User attributes from SAP S/4 On-premise and Cloud Applications

To efficiently manage synchronized users and reduce the number of users handled by IAG, you can now filter data by specific user attributes from the SAP S/4 On-premise and Cloud applications during repository synchronization in SAP Cloud Identity Access Governance.

Details



Description: S/4HANA on-premise

Application type: SAP S/4HANA On-Premise

External Application ID:

HCP Destination:

Alias:

Business Function Groups

Audit Log

User Attribute

From

Add User Filter

User Attribute *
User ID

From Value *

To Value

Scope *
Exclude

Save

Cancel

Users (3)


↓ Monitored Users


prashanth

X

Q

Prashanth Kumar Duvva

Application: 

User ID: 


>

License Metric Verification

Provides a download option in Maintain User Data app to download all unique active users monitored by SAP Cloud Identity Access Governance for licensing calculation.

Retention Policies		
Configuration Parameter	ILM Object Name	Retention Period
MANAGE_RETENTION_POLICIES	Privileged Access Logs	<div>never</div>
MANAGE_RETENTION_POLICIES	Access Request	<div>never</div>
MANAGE_RETENTION_POLICIES	Role Designer	<div>NEVER</div>
MANAGE_RETENTION_POLICIES	Access Analysis Audit Log	<div>NEVER</div>
MANAGE_RETENTION_POLICIES	Access Analysis Change Log	<div>NEVER</div>
MANAGE_RETENTION_POLICIES	Manage Job Log	<div>NEVER</div>
MANAGE_RETENTION_POLICIES	Access Certification Campaign	<div>NEVER</div>

<



Manage Jobs ▾

Create New Job


General Settings		Schedule Settings
Job Name: *	<input type="text"/>	Execution Type: <input checked="" type="radio"/> Run Immediately
Job Category: *	<div>Data Deletion ▾</div>	<input type="radio"/> Repeated Run
ILM Object: *	<div>▾</div>	<input type="radio"/> Single Run
Job Mode:	<div>Test ▾</div>	
Business Purpose:	<div><div>TestSimulation</div><div>ProductionData Deletion</div></div>	
Send Notification:	<input checked="" type="checkbox"/>	

Data Retention Management (Beta)


IAG now supports Data Retention Management.

IAG_Data_Controller_Data_Retention_Management


<



Manage User ID Mapping ▾

 PKD

Standard ▾

 ▾

Search

Q

Application:

Updated By:

Go

Adapt Filters

^

↗


User ID Mapping Entries (52)

Select by Master User ID

Create Mapping


Upload


Delete



≡

=



 ▾

Manage User ID Mapping app

The Manage User ID Mapping feature offers an improved user experience, enabling you to create and delete User ID mappings directly in the app and download mapping reports.

Access Analysis Service

Standard ▾



User ID:

Rule Set:

Risk:

Application:

Function:

Access:

Mitigated Risks:

☒ Include

Mitigation Control:

Select Control ID

<input checked="" type="checkbox"/>	MC_BC_DEMO MC for BC risks	MC_BC_DEMO
<input type="checkbox"/>	MC_FI_DEMO MC_FI_DEMO	MC_FI_DEMO
<input type="checkbox"/>	ZBB_MIT01 ZBB_MIT01	ZBB_MIT01
<input type="checkbox"/>	ZMIT1 Mitigation Control1	ZMIT1
<input type="checkbox"/>	ZSAC SAC Mitigation Control	ZSAC
<input type="checkbox"/>	ZSAC02 SAC Control 02	ZSAC02
<input type="checkbox"/>	ZSAC03 SAC Besipielkontrolle	ZSAC03

Select Cancel

Analyze User Access Enhanced Report (Access Analysis)

To perform a comprehensive risk assessment, you can now incorporate mitigated risks and control information into your search options and subsequently report them.

< **SAP** Tenant Settings ▾

Tenant Settings (2)

Search

Customer Owned Document Management Service Configuration

Subaccount Destination Name for Document Service

Security Settings

Security Settings for the Tenant

Security Settings

GENERAL INFORMATION

Description: Security Settings for the Tenant

Name: Tenant Security Settings

Created By: system-internal

ATTRIBUTES

Attribute	Value
Use Secure Storage for Reports	Active

Use Secure Storage for Reports

Name: Use Secure Storage for Reports

Description: Redirect report downloads to configured secure storage (DMS setup required)

Created By: system-internal

Active: ☒





Secure Storage of Reports on a Customer-Owned Document Server



Analyze User Access downloads can now be directed straight to your organization's Document Management Service (DMS). Each report is stored in accordance with your retention and classification policies, removing the need for manual file handling and keeping sensitive data securely within your content repository. Keep an eye on the roadmap as this feature will be extended to include other report types in future releases.

< **SAP** Document Management Service ▾ SC

Document Management Service / SecureStorage-DEMO / 2025-05-14

Standard ▾ Items (12) Search

Create ▾ Edit Link Download Delete Move Copy Manage Document ▾    

<input type="checkbox"/>	Type	Name	Modified On	Created By	Modified By	Size	
<input type="checkbox"/>		10100511_CB9980001600_20250514_0602.zip	May 14, 2025			593 KB	...
<input type="checkbox"/>		4059532_rsmiths_20250514_0600.zip	May 14, 2025			2 KB	...



Upload Rules

Description: To generate rules for your logical systems, upload a Rules zip file.

Rules File:

C.

Brow

Upload & Process

Reset Status

Refresh Status

Processing status:



Job completed on Wed Oct 04 2023 17:12:55 GMT+0200 (hora de verano de Europa central).

Log Report:

Download Processing Log

Download Validation Log

Download Rules

Description: To get a zip file of the current rules in the app, select a business function group and click Download File.

Business function group:

ALL



Action:

Download File

Updated Rulesets for Concur & BTP Financial Applications

New segregation-of-duties rulesets for Concur (Expense, Invoice, Request), SAP S/4HANA and SuccessFactors core transactions, and BTP's advanced financial-closing processes, so you can detect and manage cross-system risks with greater precision and enforce compliance consistently across your finance and HR applications.

Mitigation Control Assignments

Category: *

Select Control Category ▾

User
Access
Business Role

User:

Search Users

Application:

Risk:

Control:

Status:

All ▾


Go

 Adapt Filters



Control Assignments (0)


+ Add


 Delete

Change Validity To

Activate

Deactivate






<input type="checkbox"/>	User	Application	Risk	Risk Level	Control	Valid From	Valid To	Monitor Group	Status
--------------------------	------	-------------	------	------------	---------	------------	----------	---------------	--------

Mitigation Control Assignments

You can now select categories such as User, Business role and Access to add or modify or delete any user or role level mitigation assignments.

<



Access Analysis Audit Log Report ▾

🗨️

PKD

Access Analysis Audit Log Report

Category: *

Select Access Analysis Audit Log Category ▾

Remediation

User Mitigation Control Assignment

Access Mitigation Control Assignment

Business Role Mitigation Control Assignment

Go

Adapt Filters


⬆️

📌

Access Analysis Audit Log Report

In the report, you can view the log details relevant for Remediation, User Mitigation Control Assignment, Access Mitigation Control Assignment and Business Role Mitigation Control Assignment.


<



Mitigation Control


▼

7 Controls




6

Active



0


Draft



1

Deactivated

Controls (7)



Delete

Search

Q

Name	Description	Last Updated	Updated By	Status
<div><div><input checked="" type="checkbox"/></div>MC_BC_DEMO</div>	MC for BC risks	May 20, 2025, 6:40:59 PM	<div></div>	Active >
<div><div><input checked="" type="checkbox"/></div>MC_FI_DEMO</div>	MC_FI_DEMO	May 20, 2025, 6:48:40 PM	<div></div>	Active >
<div><div><input checked="" type="checkbox"/></div>ZBB_MIT01</div>	ZBB_MIT01	May 27, 2025, 5:52:15 PM	SYSTEM	Active >
<div><div><input type="checkbox"/></div>ZMIT1</div>	Mitigation Control1	May 27, 2025, 5:52:14 PM	SYSTEM	Active >

Delete Functionality for Master Data Configuration

To manage and update system settings effectively, you can now delete functions and controls in the Control Master Data.

PUBLIC

You can now synchronize SAP BTP authorizations and perform Segregation of Duties (SOD) by extracting and evaluating data-level authorizations for BTP application roles and users.

Create Destination for Data-Level Extraction

To synchronize SAP BTP authorizations and for a comprehensive and accurate SoD analysis, you can effectively extract and analyze data-level authorizations for BTP application roles and users.

You can extract the following data via the existing SAP BTP synchronization job:

- **Role-Based Data Authorization:** The system allows you to extract data-level authorizations for all BTP (Business Technology Platform) application roles. This includes detailed information about the permissions and data access levels assigned to each role.
- **User-Specific Authorization:** The system enables the extraction of data-level authorizations for individual users based on their assigned BTP application roles.
- **Scheduled Extraction:** The system allows the scheduling of regular data extraction processes, ensuring that up-to-date data is available for ongoing SoD analysis.

Access Request Service

The dynamic risk owner determination relies on the following attributes:

Risk Attributes:

- riskId: Risk ID
- riskLevel: Risk Level
- riskBusinessProcess: Risk Business Process

User Attributes:

- department: Department
- company: Company
- userGroup: User Group
- jobCode: Job Code
- location: Location
- division: Division
- plant: Plant



[Manage Projects](#) / [IAGWorkflowBusinessRule](#) /

RiskOwnerRule



Import

Export

Edit

Validate

[Details](#)

[Decision Table](#)

Decision Table

Decision Table

If	Then
riskLevel of the RiskOwnerAttributes is equal to	ApproverId
'3'	'P000637'
'1'	'P000098'
'2'	'P000631'
'0'	'P000102'

Dynamic Risk Owner Determinator

Dynamic determination of the risk owner stage approver is an additional workflow type for Business Rule Framework, which is for assigning approvers to risk owner stages in access requests. This determinator assigns the risk owners based on business rules that evaluate both risk and user attributes when an access request is created.

Conditions / attributes of access on which auto approval rules can be based:

- 1. Role name
- 2. Role criticality/Business role criticality (Low, medium, high and critical)
- 3. Role approver
- 4. Role business process
- 5. Role sub process
- 6. Role risk count

Line item auto approval at role owner stage

This functionality allows for automatic approval of access request line items during the role owner stage.

Decision Table

Decision Table

If	Then
roleCriticality of the RoleOwnerAttributes is equal to	roleOwnerAutoStage
'Low'	true

Review Request

Request Details Access Requested User Details Attachment

FSN Connector All

S44

Single Role

User Details

Job:

User Group:

Company:

Location:

Division:

Position:

Language:

Department:

Organizational Unit:

Access Request Form Header

When creating an access request, you can now view additional user attributes in Create Access Request and Creating Access Request for Others apps.

Access Request Demo

▼

Access Requested	Existing Assignments	Additional Details	User Details	Attachments	Notes	Audit
Access	Access Type	Action	Validity Period	Risks	Approve or Reject Access	
<div>Bank Maintenance</div> <div></div>	Single Role	Add		<div>⚠️ 1</div>	<div><div><input type="radio"/></div> Approve</div> <div><div><input type="radio"/></div> Reject</div>	
<div>Payment Processing</div> <div></div>	Single Role	Add		<div>⚠️ 1</div>	<div><div><input type="radio"/></div> Approve</div> <div><div><input type="radio"/></div> Reject</div>	

Request Administration app

This app now allows administrators to approve requests at any stage for absent approvers or delegates.

Request Delegation ▾

PKD

Standard ▾

Status Type:Valid From:Valid To:Updated On:

Search

Select Status ▾

e.g. 12/31/25

e.g. 12/31/25

e.g. 12/31/25

Add Delegation

Approver*	Delegatee*	Valid From*	Valid To*	Status*
<div>P000089</div>	<div></div>	<div>Please select valid from... </div>	<div>Please select valid to d... </div>	<div>Active ▾</div>

Save

Close

Request Delegation app

This app helps you to delegate your access requests to other approvers or delegates if you are not available for a certain period.

Access Certification Service

<

SAP

Campaign Results ▾

PKD

Standard* ▾

🔗 ▾

Search

Q

All Items Approved:

All ▾

Close Date:

🔍

Go

Adapt Filters (1)

⬆️ ⬇️

Campaigns

⚙️ 📅 ▾

Name	Description	All Items Approved	Close Date	
No data found. Try adjusting the search or filter criteria.				

Campaign Results app

With this app, you, as access certification users, can view and review decisions relating to closed campaigns.

Privilege Access Management Service

3389398 - Security Vulnerability:
Standard SAP User Able to Modify PAM
User Master Data.

3389398 - Security Vulnerability: Standard ...

SAP Note, Version: 9, Released On: 14.03.2025

- Description
- Software Components
- Correction | v
- Support Package
- Attributes
- Available Languages

Symptom

When administrator setting up a User type Dialog in the SAP system to assign a PAM ID for connecting to the managed SAP system through the SIAG_PAM_LAUNCH_PAD, a potential security issue could occur. This issue arises when the User type Dialog has rights to change user master data. Most critical change is the passwords reset for the PAM User (User type Service). If this happens, the User type Dialog could potentially misuse a PAM User login credentials for unauthorized access to the system.

Privileged Access Monitoring Report

For PAM requests, two new columns and filters called Reviewer and Stage have been introduced. PAM log review requests that are in pending status can be processed by various reviewers. In addition, administrators have an overview of PAM log review requests in the Pending status.

In addition, to ensure continuity of workflow and to maintain accurate audit trails, you can now forward PAM log requests to another reviewer.

Privileged Access Logs (23)

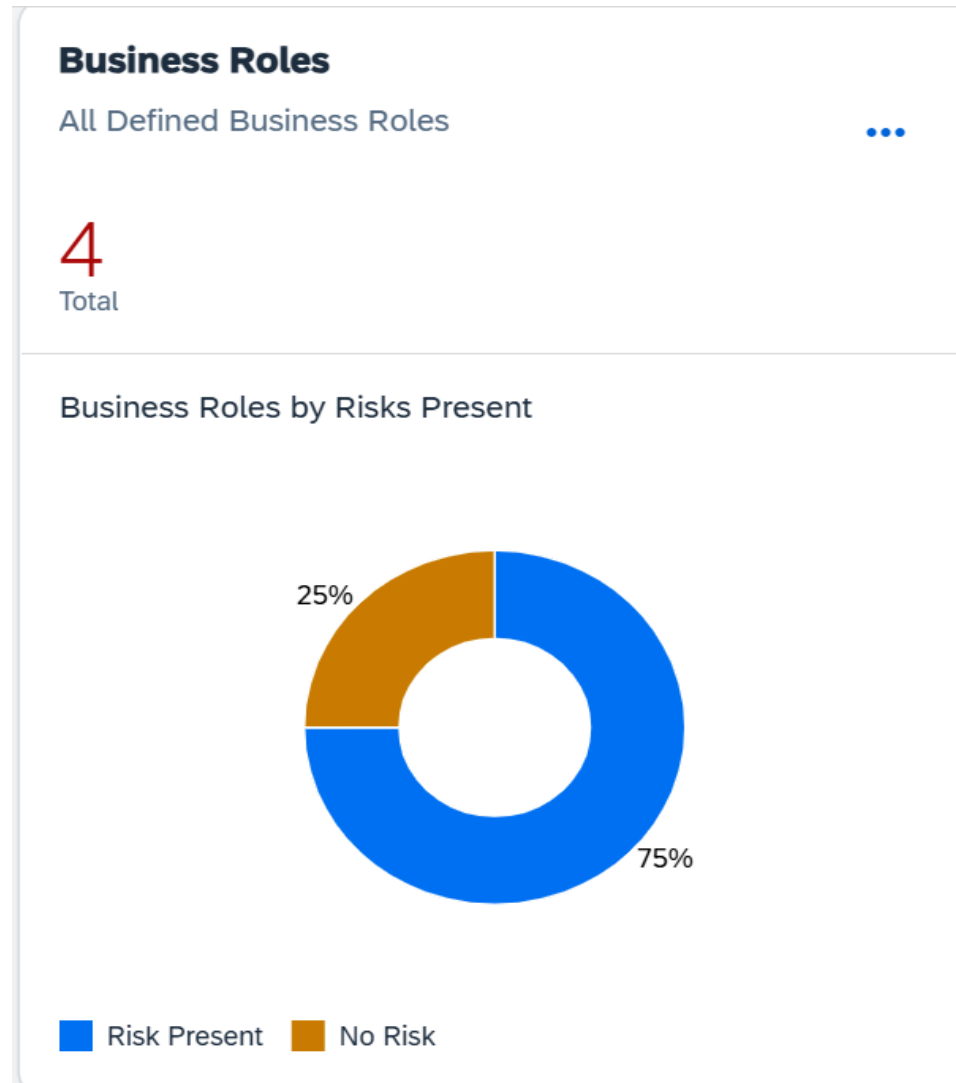
Forward    | 

<input type="checkbox"/>	Privileged Access ID	Duration (DD:HH:MM:SS)	Request Number	Status	Reviewer	Stage	
<input checked="" type="checkbox"/>	PAMID_DEMO08	00:00:01:53	PAM23	Pending		Security	>
<input type="checkbox"/>	PAMID_DEMO08	00:00:02:02	PAM22	Pending	1 Reviewer	Role Owner	>
<input type="checkbox"/>	PAMID_DEMO7	00:00:07:22	PAM21	Pending	1 Reviewer	Role Owner	>
<input type="checkbox"/>	PAMID_DEMO6	00:00:00:42	PAM20	Pending	5 Reviewers	Security	>
<input type="checkbox"/>	PAMID_DEMO5	00:00:00:00	PAM19	Pending	1 Reviewer	Role Owner	>

Role Design Service

Role designer overview dashboard

Introduced a new category called Risks that lists all the risks identified for a particular business role. This allows you to directly mitigate a particular risk based on your authorization in Edit mode.



References

- ❑ What's New for SAP Cloud Identity Access Governance

https://help.sap.com/docs/SAP_CLOUD_IDENTITY_ACCESS_GOVERNANCE/e739622ded9b4d92964c6a0f50b5f90e?locale=en-US&state=DRAFT&version=DEV

- ❑ Administration Guide for SAP Cloud Identity Access Governance

https://help.sap.com/docs/SAP_CLOUD_IDENTITY_ACCESS_GOVERNANCE/e12d8683adfa4471ac4edd40809b9038?locale=en-US&state=DRAFT&version=DEV

- ❑ 3389398 - Security Vulnerability: Standard SAP User Able to Modify PAM User Master Data

- ❑ Role owner stage auto approval in IAG

<https://community.sap.com/t5/technology-blog-posts-by-sap/role-owner-stage-auto-approval-in-iag-access-request-service/ba-p/14101290>

Q&A

Thank you.

Contact information:

Name Prashanth Kumar Duvva

Email prashanth.kumar.duvva@sap.com



Follow us



www.sap.com/contactsap

© 2025 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See www.sap.com/copyright for additional trademark information and notices.