

From Chaos to Control – How Jabil Automated User Access Reviews Across Multiple SAP Landscapes

Susan Zortea, Governance Lead, Jabil
Hannah Sears, SAP Controls Specialist, Jabil

Las Vegas

2024

SAPinsider



In This Session

- Learn how to navigate process design decisions related to moving access review processes for multiple production systems into GRC Access Control.
- Understand the benefits of leveraging Access Control to automate access reviews.
- Establish future-state governance processes.
- Discuss lessons learned
- Identify and leverage key metrics to measure value and success.

What We'll Cover



About Jabil



Our SAP Environment



Legacy Process Pain Points with Access Reviews



Future State Processes We Designed and Implemented



Lessons Learned



KPIs We Used To Measure Success



About Jabil

In this section we'll provide an overview of our organization.



Jabil Today: Built on a Solid Foundation

50+

YEARS OF CROSS-INDUSTRY
EXPERIENCE

140K+

DEDICATED
EMPLOYEES

\$34.7B

REVENUE
IN FY23

\$30B

GLOBALLY MANAGED
SPEND

36K+

SUPPLY CHAIN
PARTNERS

400+

CUSTOMERS ACROSS
DIVERSE MARKETS

100+

SITES STRATEGICALLY LOCATED
AROUND THE WORLD

25+

COUNTRIES

41M+

SQUARE FEET OF
MANUFACTURING SPACE

Global Operations Enable Manufacturing at Scale

100+ Sites

Strategically Located Around the World

ASIA

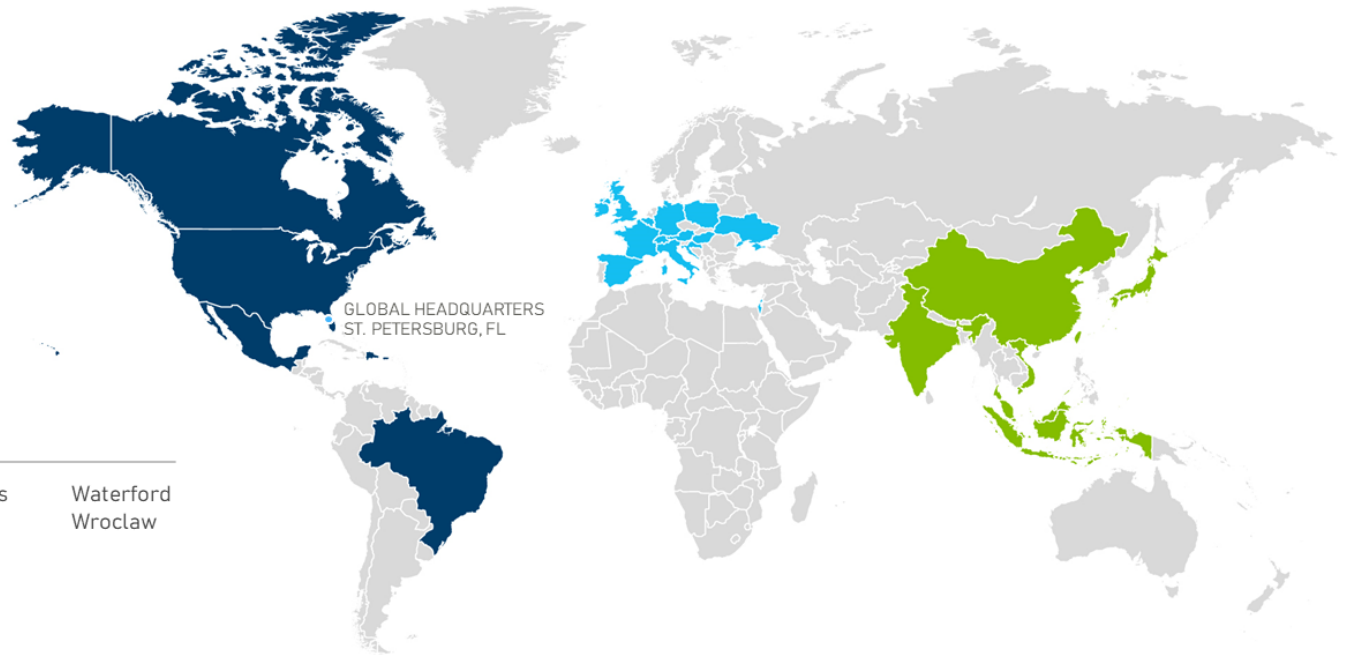
Bandung	Hachioji	Neihu	Shenzhen	Tianjin
Batu Kawan	Ho Chi Minh	Penang	Singapore	Weihai
Beijing	Hsinchu	Pune	Sungai Petani	Wuhan
Changhua	Huangpu	Sanchong	Suzhou	Wuxi
Gotemba	Kulim	Shanghai	Taichung	

EUROPE & MIDDLE EAST

Balsthal	Dublin	Kharkiv	Mezzovico	Tiszaújváros	Waterford
Bar-Lev	Grenchen	Kwidzyn	Nagyigmánd	Tortosa	Wroclaw
Bettlach	Hägendorf	Livingston	Osijek	Tuttlingen	
Bray	Hasselt	Le Locle	Paris	Uzhgorod	
Coatbridge	Jena	Marcianise	Raron	Vienna	

AMERICAS

Albuquerque	Auburn Hills	Burlington	Chihuahua	Grand Junction	Juarez	Maple Grove	Monterrey	Pleasanton	San Jose	Valinhos
Anaheim	Austin	Cayey	Clinton	Guadalajara	Lexington	McLean	Monument	Richardson	Santo Domingo	Vancouver
Asheville	Belo Horizonte	Chaska	Florence	Gurnee	Manaus	Mebane	Mount Pleasant	Richmond	St. Petersburg	West Chester
Atlanta	Benicia	Chicago	Fremont	Hanover Park	Manteca	Memphis	Ottawa	San Cristobal	Tijuana	



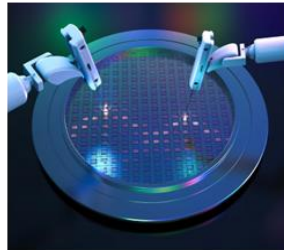
Tailored Solutions Backed by Cross-Industry Expertise



5G
Wireless



Automotive &
Transportation



Capital
Equipment



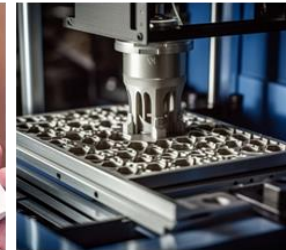
Cloud
Infrastructure



Connected
Devices



Digital
Commerce



Digital
Print



Defense &
Aerospace



Healthcare



Energy Storage
& Management



Networking
& Storage



Optics



Packaging



Renewable
Energy



Smart Home
& Appliances



Warehouse
Automation

About Jabil

- In this section we will provide an overview of our SAP landscape.
- We'll also provide an overview of our GRC landscape.



Our Current SAP Landscape

We have seen tremendous growth in our business as well as growth through acquisition which has led to a much more complex landscape than our single SAP landscape, we lived in many years ago.

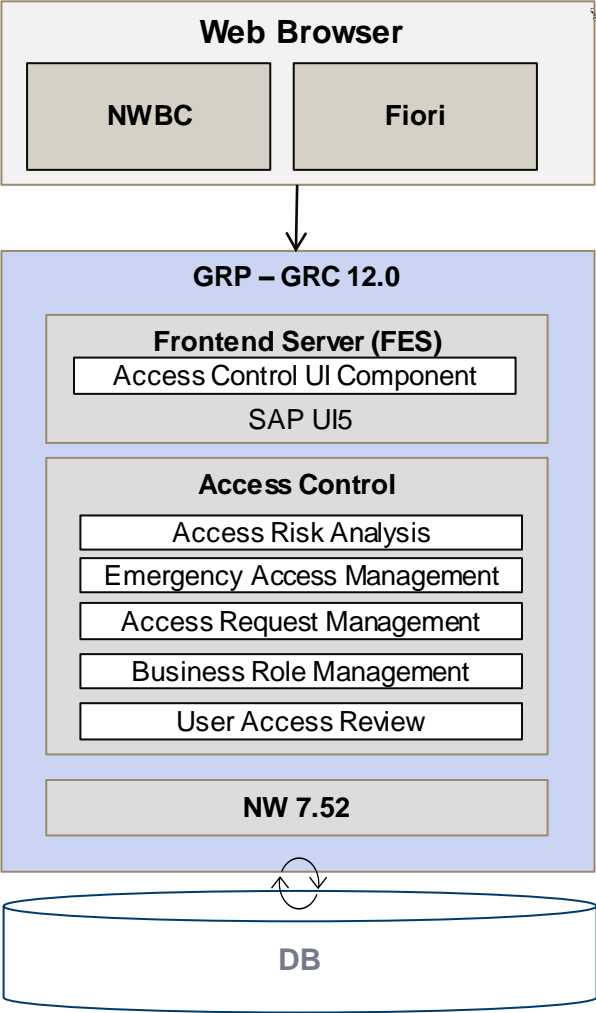
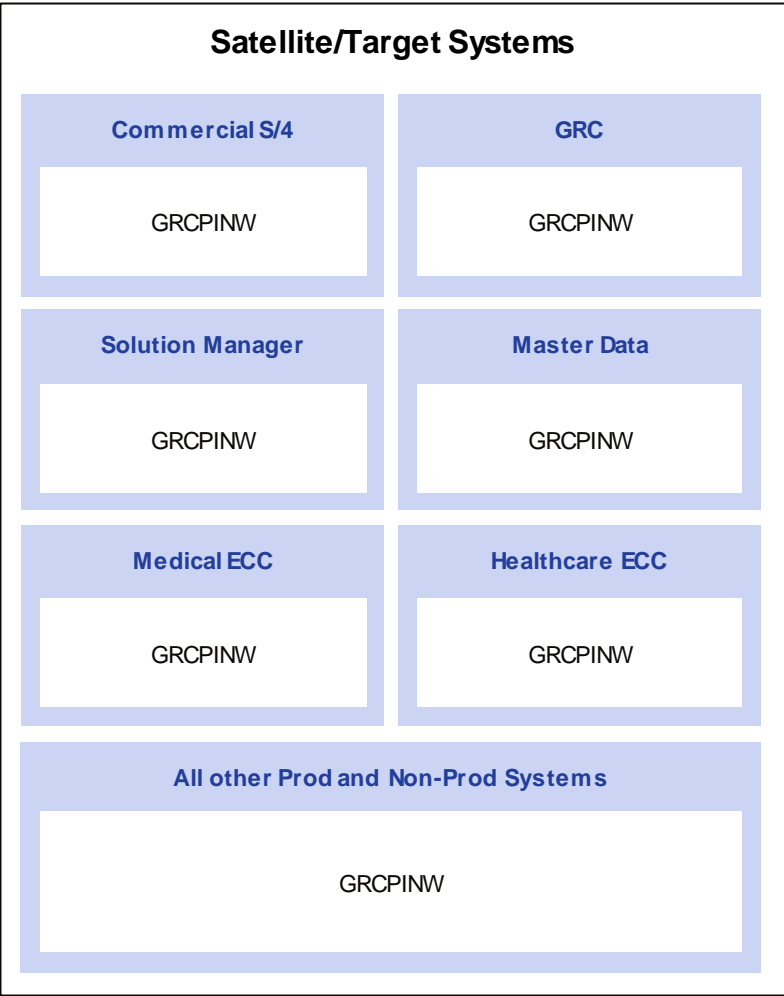
SAP Systems	Active Users	Comments / Notes
S/4HANA (Commercial)	~36,000	Recently upgraded to S/4HANA
ECC (Nypro Healthcare)	~4,200	S/4HANA upgrade planning in process
ECC (Medical)	~4,000	S/4HANA upgrade planning in process
GRC	~15,000	Upgraded to SP14 May 2022, planning upgrade to latest SP in 2024
MDG	~4,500	-
Solution Manager (SOLMAN)	~900	-

GRC Architecture and Landscape

- GRC Access Control 12.0 with limited functionality implemented for Process Control.
 - A 3-tiered + 1 landscape with sandbox system.
- Access Control is connected to production and non-production systems.
 - Access provisioning is configured to sandbox, development, staging and production systems across multiple SAP clients.
 - Over 90 connectors!
- We deployed all core functionality in Access Control but were not using UAR until this project.



Production Technical Landscape Diagram



RFC





Scope and Legacy Processes Pain Points

In this section we will discuss:

- Overview of our legacy processes
- Pain points associated with the legacy processes.
- Scope of controls which were being impacted.

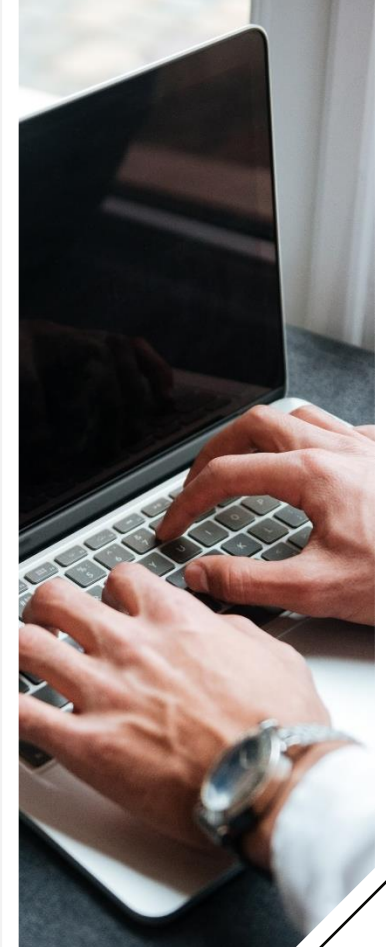


Scope of Controls

Control Area	Risk Statement	Example Control Description
 User Access Review (UAR)	The risk of end user accounts having inappropriate access within SAP.	A review of dialog user accounts is performed by the user's manager to ensure that users have the appropriate access according to their job responsibilities.
 Critical Transaction Access Review (CTAR)	The risk of a user having critical access in production	A review of SAP dialog and service user accounts must be performed to ensure the appropriateness of access to critical transactions.
 Critical Transaction Execution / Usage Review (CTER)	The risk of user and generic non-human accounts executing critical access in SAP (e.g., SAP_HELP)	A review of the critical transactions executed by SAP dialog and service accounts is performed to ensure that their usage was appropriate.
 Firefighter Session Review (FFSR)	The risk of elevated access being performed without a timely detective review .	A review of the Firefighter activity logs is performed by Firefighter Controllers for Firefighter ID use in the production environment.

Pain Points from Legacy Process

- **Extensive hours of manual report manipulation**, with formulas in excel to find Managers, Manager User IDs, filter out certain criteria (e.g., removing generic access).
- **Manual communication** reminders
- **Detailed documentation and reports for audit** (multilayer excel files that captured every step of the process)
- Required to **manually submit various tickets** for the different type of removal scenarios.
- **Manual access removal process** for the security team would take at least a week.
- **Disconnect between systems due to the lack of data synch**. Managers wouldn't be in Quality but would be in Production.
- **Time was needed for testing the workflow each review** through development, staging/QA and production before launching the review.
- **Lack of resources with knowledge of the legacy tool** due to its age.



User Access Review (UAR) Automation

In this section we'll cover:

- Future state UAR process
- Key design decisions
- Overview of the process flow
- UAR prerequisites
- Completeness and accuracy checks
- Lessons learned





Overview of GRC UAR Automation

We evaluated various tools from other vendors and agreed on moving forward with GRC Access Control.

Leveraged our existing SAP GRC Access Control system to support the process with an automated workflow-based review and approval.

Access Control offers the following improvements from our current state:




- 1 Centralized and automated process for periodic access review
- 2 Automated removal of access, reducing reliance on additional tickets and SAP security resources
- 3 Ability to centrally monitor status of the reviews
- 4 Audit trail and reports for supporting audit teams
- 5 Reduction in manual tasks to improve control performance
- 6 Increased effectiveness and visibility to incomplete user access reviews





Participants in the UAR Process

GRC includes the following participants that can appear in UAR:

GRC Role	Description of Responsibilities	Jabil Resource Responsibility
 UAR Administrator	Administrators will perform UAR-specific administration tasks, such as generating, cancelling and regenerating UAR requests for rejected users. Administrators will also perform admin reviews before generating a workflow for the request.	SAP COE Governance Team
 UAR Reviewer	Approvers at the Reviewer stage. The direct manager of a user, as defined in Active Directory as the source.	User's Direct Manager
 Coordinator	Users assigned to Reviewers. Coordinators monitor the UAR process and coordinate activities to ensure that the process is completed in a timely manner.	SAP COE Governance Team

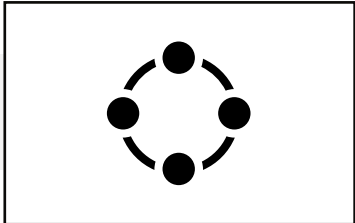


Process Design Decisions

Design Decisions	Configuration Parameter ID
1 Manager will perform review	2006
2 Notifications sent to end user when access removed	2062
3 One UAR request per Reviewer with all users in request	2064
4 The GRC Admin will review the requests before sending out	2007

Param ID	Parameter Value	Description
4018	YES	Enable detailed logging (SLG1) for EAM Log Synchronization programs
4020	YES	Generate EAM log for Firefighter sessions with no activity
4025	YES	Restrict Firefighter Validity period during Access Request
4027	NO	Set Ticket selection to mandatory in EAM Logon Pad
5033	NO	Allow Firefighters with no controller
2004	011	Request Type for UAR
2005	009	Default Priority
2006	MANAGER	Who are the reviewers?
2007	YES	Admin. review required before sending tasks to reviewers
2008	500	Number of line items per UAR request
2062	YES	Send notification to users whose access is removed
2063	YES	Show approved lineitems in UAR Audit Log
2064	NO	One UAR request per user
2065	NO	Allow reviewer to approve own assignments
1120	1000	Batch size for Batch Risk Analysis
1121	1000	Batch size for User sync
1122	1000	Batch size for Role sync
1123	1000	Batch size for Profile sync
2050	YES	Enable Realtime LDAP Search for Access Request User.

IMG Configuration Path: GRC → Access Control → Maintain Configuration Settings



Process Design Decisions

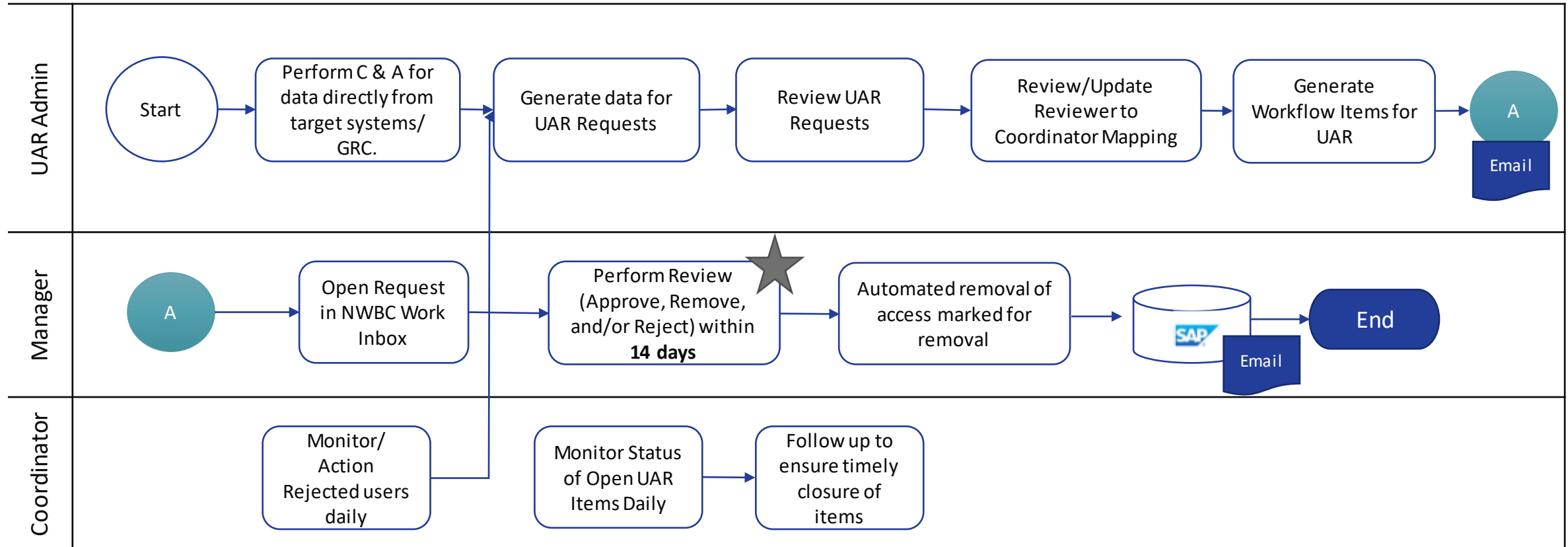
	Design Decisions	Configuration Area
1	Coordinator for all review items will be SAP COE Governance team	Process Design
2	SAP security team will not be included in the review process	Workflow Config
3	Separate review for each system (large data volume)	Process Design
4	Users with failed login locks will be included in the review	Plug-in Config Parameter
5	Reviewers cannot forward request	Workflow Config
6	Request will not be escalated but reminder emails will be sent to Managers after 2 days	Workflow Config
7	Review due 14 days after review request is sent	SLA Config



UAR Process Flow

UAR Process will now be managed within SAP GRC Access Control

Workflow based review sent to Managers for review of roles assigned to users for key SAP systems



UAR Prerequisites

Sync Jobs

- The below sync jobs must also be executed in sequence for all in scope connectors before generating UAR requests, however, all of these jobs are scheduled to run incrementally and as full syncs and is managed by the job scheduling tool.
- The Repository Object Sync needs to be executed for the LDAP connectors prior to generating the UAR. A full sync for these connectors have to be run prior to generating the UAR data.
- The job populates users that are included in the UAR and the Managers data in the GRC repository (table: GRACUSER).

Role Maintenance / Import

- Any role assigned to a user in the target system must be imported into BRM in order for the assignments to be included in UAR.
- Critical level of roles that need to be included in UAR have to be marked as High criticality (value of Low is excluded).
- Methodology status has to be Complete.
- Provisioning settings must be set to Yes.



Reviewer Account Status

- All reviewers synchronized as Managers (GRACUSER) must have an active and valid user account within GRC Production (USR02).



UAR Criteria

	Filter Criteria	Value	Comments
1	Connector ID		Select by connector ID
2	Critical Level	High	Excludes low risk roles which are currently auto approved
3	Excluded Expired Users	Yes	Based on user validity dates
4	Excluded Expired Roles	Yes	Based on role validity dates
5	Exclude Locked	Yes	Yes – excludes all lock values, except failed login locks No – includes all locked users
6	User Type	Dialog	Include only end user accounts with Managers

Note: Non-human IDs will not be included; these are covered as a separate review



UAR Criteria

Scheduler

Create Schedule

Schedule Name UAR C&A Analysis - P02 Schedule Activity Generates data for access request UAR review

1 Schedule Details 2 Select Variant 3 Review 4 Confirmation

Saved Variants:

Connector Id	is		+ -
Critical Level	is	High	+ -
Exclude Expired Users	is	Yes	+ -
Exclude Expired Roles	is	Yes	+ -
Exclude Locked Users	is	Yes	+ -
User Type	is	Dialog	+ -

Clear Save Variant As: Save

Previous Next Cancel Finish Close

Completeness and Accuracy Checks



Why?

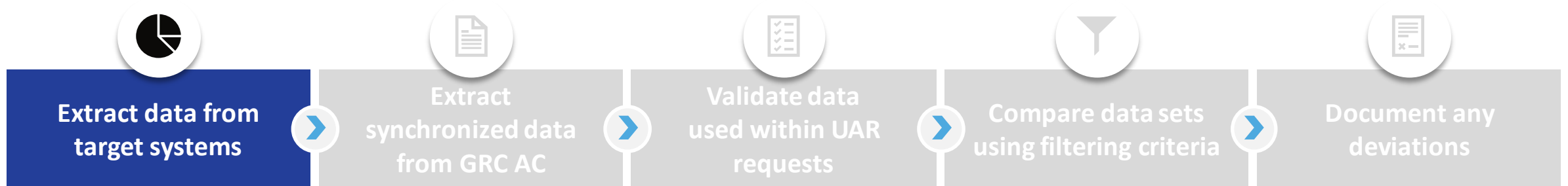
- Confirm that all user and role assignments are being included in the review process
- Ensure we can demonstrate this to audit



Our Challenge:

- The UAR process we have designed leverages Manager as the reviewer
- This configuration relies on Active Directory
- **Important:** The Access Control UAR functionality for reviewing access starts with role data synced into AC – it does NOT start with what is in the target systems.
- **Also Important:** Synchronization jobs are critical to completeness; if they're not working correctly then there will be gaps in the UAR data collection and review.

Completeness and Accuracy Checks

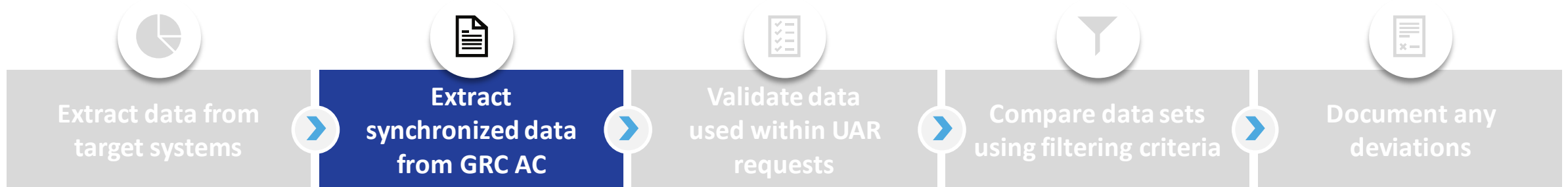


Key tables to extract from target systems:

- USR02 – table of users, user type, and user lock status
- AGR_USERS – table of user to role assignments
- Apply Filter Criteria for User Type=Dialog (A); Users which are not locked



Completeness and Accuracy Checks



Key tables to extract from GRC AC system:

- 1 USR02 - table of users, user type, and user lock status
- 2 GRACUSER – user master record for list of users from LDAP connector(s)
- 3 GRACUSERCONN – user details by system connector
- 4 GRACROLE – roles which are imported into GRCAC BRM module with role ID and name by connector group
- 5 GRACREQ – request numbers to request ID relationship filtered by Job ID
- 6 GRACREVITEM – table with request ID, user ID, and role ID
- 7 GRACREVCORDMAP – table with reviewer to coordinator mapping

Completeness and Accuracy Checks



Validation Checks:

- 1 To identify and validate the user lock status between the target system and GRC
- 2 Precheck No. 2: To identify and validate the user validity date between the target system and GRC
- 3 Precheck No. 3: To identify and validate the roles in GRC Business Role Management (BRM) (e.g., critical level, provisioning status)
- 4 Precheck No. 4: To identify users that are not in Active Directory
- 5 Precheck No. 5: To identify managers of users that are not in Active Directory
- 6 Completeness & Accuracy (C&A) Check: To identify if a User-Role Assignment is missing from the UAR data
- 7 Exclusions for generic IDs or other accounts which will not be part of this UAR process.

Important: Investigate and document any deviations since; timing of jobs and analysis created variances in our largest system due to the volume of access changes.

Password Parameters

We made a design decision to include users with failed password locks will be included.

Note: This is configured with parameter 1004 on each target (plug-in) system.



Table View Edit Goto Selection Utilities System Help

Display View "For System Details": Overview

For System Details

Param Id	Sequence	Parameter Value	Short Description
1000		GRPLNT010	Please maintain Plug-in Connector
1001	0	GRPLNT010	Please maintain GRC connector
1004	0	128	User Lock Type to be excluded in Repository Sync
1090	0	ZS_GRAC_SPM_FFID	FFID Role Name
4000	0	1	Application type
4001	0	99999	Default Firefighter Validity Period (Days)
4008	0	NO	Send FirefightId Login Notification
4010	0	ZS_GRAC_SPM_FFID	Firefighter ID role name

IMG Configuration Path: GRC (Plug-in) → Access Control → Maintain Plug-In Configuration Settings

UAR Lessons Learned

1

Need to actively monitor UAR requests that are rejected to ensure deadlines can be met

- A rejected request is created as a new UAR request with a new due date from the date of creation

2

Verify managers are unlocked and valid prior to launch.

3

Consider the end user experience and accessing GRC consistently (e.g., we have multiple entry points through portals, Fiori, and NWBC)

4

How to handle completeness and accuracy

5

Active Directory synchronization and relationship to GRC system

6

How to address non-human IDs

7

Importance of accurate user and role master data (e.g., criticality of roles, manager data, etc.)

UAR Lessons Learned (Continued)



Manual communication plan / escalation.



An SAP popup was added for users who were going to be impacted by access removal due to a missing UAR



We manually send reminders out to be able to manage the communications more specifically (days 2, 9, 15, 28)



Managers that do not complete the review will result in a force closure of the request and removal of access their team members.



Critical Transaction Access Review

In this section we'll cover:

- Future state critical transaction access review (CTAR) process
- Key design decisions
- Overview of the process flow
- Prerequisite tasks



Overview of Critical Transaction Access Review






Replacement of the current tool which was used to support the critical transaction access review (CTAR) process and was semi-automated through a workflow.

Leveraged the out of the box SOD Risk Review workflow, but tailored it for just Critical Access

We configured the ruleset with our critical access risks and utilized the existing GRC AC functionality to automate the process

Participants in the CTAR Process

GRC includes the following participants that can appear in CTAR:

GRC Role	Description of Responsibilities	Jabil Resource Responsibility
 Administrator	Administrators will perform CTAR-specific administration tasks, such as generating, and regenerating CTAR requests. Administrators will also perform admin reviews before generating a workflow for the request.	SAP COE Governance Team
 Risk Owner / Reviewer	Responsible for performing a review of user access which contains IT critical access risk as defined in the GRC ruleset.	SAP IT Director
 Coordinator	Users assigned to Reviewers. Coordinators monitor the CTAR process and coordinate activities to ensure that the process is completed in a timely manner.	SAP COE Governance Team

Process Design Decisions



Design Decision

- 1 Critical access will not be assigned to any end user accounts (exception for NW team)
- 2 Critical transaction access review will include risks defined as “Critical”
- 3 Critical transaction access review will include dialog & service accounts (excluding Firefighter IDs)
- 4 Critical transaction access review will automatically remove role(s) with critical access
- 5 Review due 14 days after review request is sent



Process Design Decisions

- Parameter 2018 was set to define the reviewer as the Risk Owner – maintain in the ruleset master data
- Parameter 2023 was set to perform the actual removal of the role with critical access.

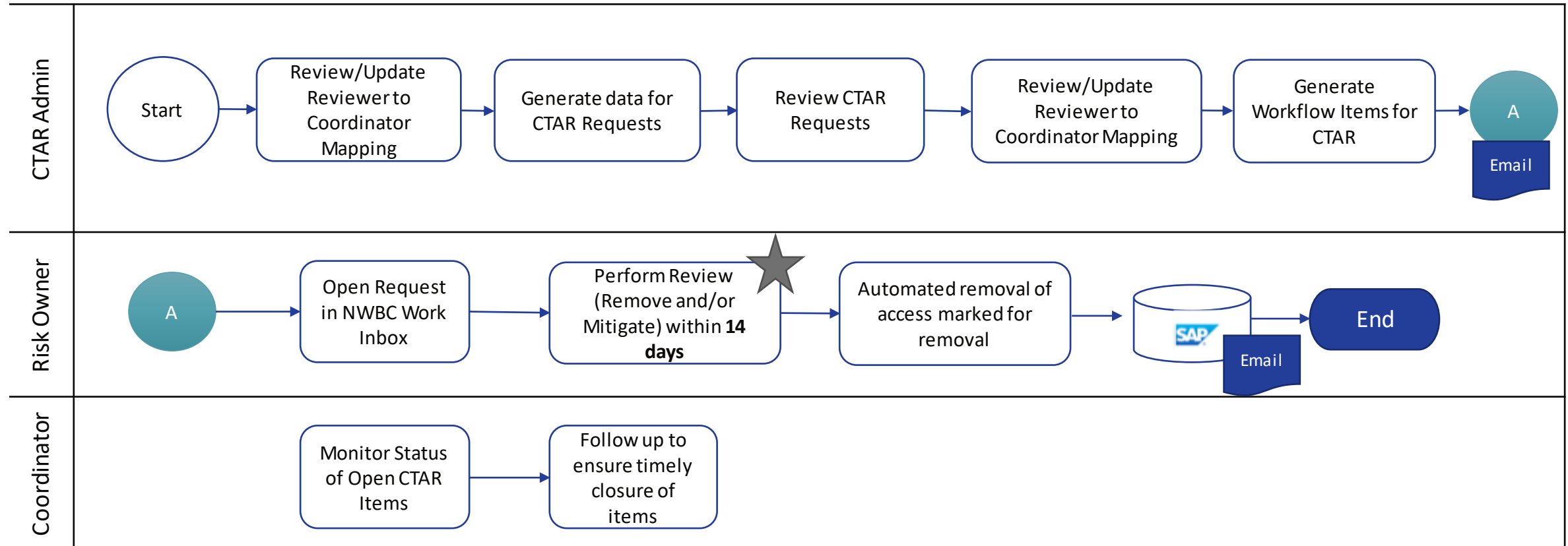
SOD Review	▼	2016	010	Request Type for SoD
SOD Review	▼	2017	015	Default priority for SoD
SOD Review	▼	2018	RISK OWNER	Who are the reviewers? ←
SOD Review	▼	2019	YES	Admin. review required before sending tasks to reviewers
SOD Review	▼	2020	9999	Number of unique line items per SOD request.(Maximum 9999)
SOD Review	▼	2021	NO	Allow reviewer to approve own assignments
SOD Review	▼	2023	YES	Is actual removal of role allowed ←

IMG Configuration Path: GRC → Access Control → Maintain Configuration Settings



CTAR Process

This process will now be managed within SAP GRC Access Control
Workflow based review of all critical access by role assigned to users



Critical Transaction Access Review Prerequisites

Sync Jobs:

- In addition to the user and role sync jobs,
- Ensure Batch Risk Analysis Job is scheduled and running

Configuration:

- The parameter for storing batch risk analysis as offline data should also be enabled (parameter 1027 – Enable offline risk analysis).
 - The job which collects the information for the workflow relies on the SOD results that are already stored in the GRC tables.

Important:

This process relies on the Batch Risk Analysis results stored within the GRC tables.

CTAR Criteria

Filter Criteria	Value	Comments
Connector ID		Select by connector ID
Access Risk ID		Critical risks (e.g., YBSA04*)
Exclude Expired Users	Yes	Based on validity dates
Exclude Locked Users	Yes	Exclude admin locked users
User Type	Dialog	Include end user accounts
User Type	Service	Include service accounts

- Criteria is defined within the scheduled job that collects the data
- Review will focus on critical risks separated by function for more granular reporting.
- This review will include dialog and service IDs, we will exclude Firefighter IDs
- Risk Owner is defined within ruleset master data and leveraged using standard workflow configuration.



CTAR Criteria

Scheduler

Create Schedule

Schedule Name Test Schedule Activity Generates data for access request SoD review

1 2 3 4
Schedule Details Select Variant Review Confirmation

Saved Variants: PRD CTAR [Delete]

Connector Id	is		+ -
Access Risk ID	is	YBSA04*	+ -
Exclude Expired Users	is	Yes	+ -
Exclude Locked Users	is	Yes	+ -
User Type	is	Dialog	+ -
User Type	is	Service	+ -

Clear Save Variant As: PRD CTAR Save

Previous Next Cancel Finish Close

- Example of the background job: **“Generate data for access request SoD review”**

Critical Transaction Usage/Execution Review

In this section we'll cover:

- Future state critical transaction access review (CTER) process
- Key design decisions
- Overview of the process flow
- Prerequisite tasks
- Ruleset design considerations



Process Design Decisions



Design Decision

- 1 Critical transaction execution review will include all users
- 2 Critical transaction execution review will include risks defined as “Critical”
- 3 Review due 30 days after review request is sent

Overview and Participants

There is currently no out-of-the-box automated workflow which will deliver the details required for the critical transaction execution review (CTER). The process will continue as-is, utilizing GRC reporting and will focus on all users who execute critical transactions, inclusive of generic non-human accounts.

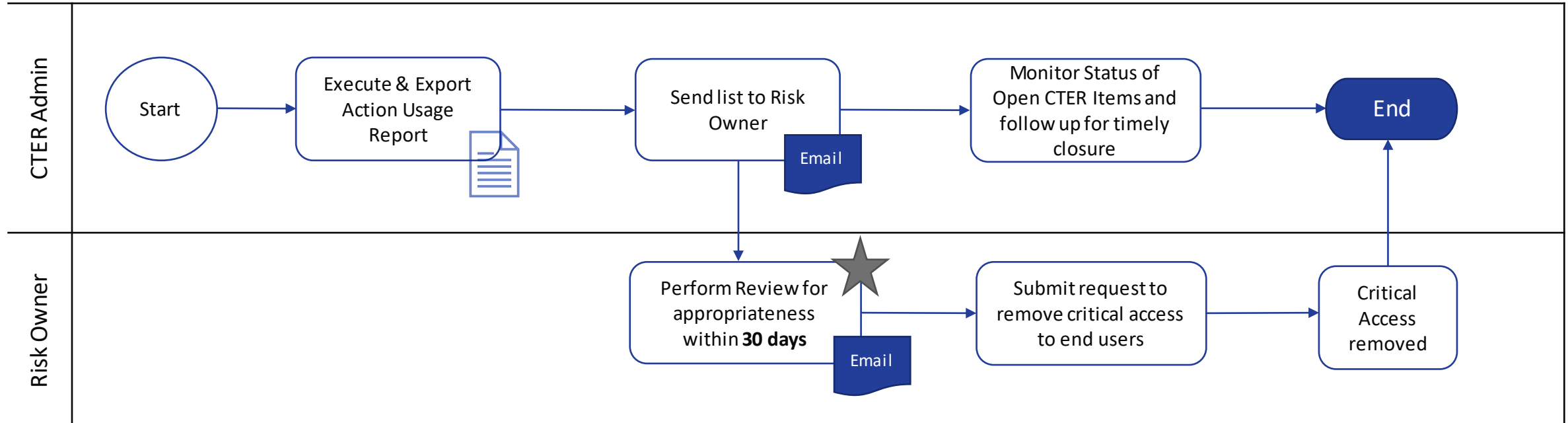
Participants in the CTER Process

GRC includes the following participants that can appear in CTER:

GRC Role	Description of Responsibilities	Jabil Team Responsibility
Administrator	Administrators will perform CTER-specific administration tasks, such as generating the report data, exporting the data.	SAP COE Governance
Risk Owner	IT Risk Owner will perform the review of critical transactions being executed. Submits request for critical access removal.	SAP IT Director

CTER Process

Review of all critical transactions executed for key SAP systems



CTER Criteria

This review process is supported using the standard Access Control report called **Action Usage by User, Role and Profile**.

	Filter Criteria	Value	Comments
1	System		
2	Action Usage Date	Date Range	Review completed quarterly
3	Report By	User	
4	Report Type	Actions Defined in Risks	
5	Access Risk ID	YBSA06	All critical access defined as a “critical action” risk

CTER Criteria

Action usage by user, role, and profile

Analysis Criteria

Saved Variants:

System is
Action Usage Date is between And

Report By: User Role Profile

User ID is

Report Type: Actions Defined in Risks All

Access Risk ID is YBSA01

Important: When selecting the Report Type value of “Actions Defined in Risks” this functionality only works if the risk is defined as a Critical Action Risk. It does not work for Critical Permission Risks.

Critical Access Risk Ruleset Design

This section provides an overview of our Critical Access ruleset design.



Sensitive Access Risk Design in GRC

Reporting Function Group	YSA01: Sensitive Access – Critical		YSA02: Sensitive Access – High
Detailed Function Group	YSA04A: Sensitive Access – ABAP Admin	YSA04E: Sensitive Access – Custom Transactions	YSA05A: Sensitive Access – Background Job Admin
	YSA04B: Sensitive Access – Archiving Admin	YSA04F: Sensitive Access – Debug	YSA05B: Sensitive Access – Table Access
	YSA04C: Sensitive Access – Client Admin	YSA04G: Sensitive Access – Role Maintenance	YSA05C: Sensitive Access – User Admin
	YSA04D: Sensitive Access – Configuration Actions	YSA04H: Sensitive Access – Transport Admin	

Sensitive Access Design - Critical Risk Function Group

Reporting Function Group	YSA01: Sensitive Access – Critical	Function Group	Action	Action Description	
	Detailed Function Group	YSA04A: Sensitive Access – ABAP Admin	YSA04A	SA38	ABAP Reporting
YSA04B: Sensitive Access – Archiving Admin		SE11		ABAP Dictionary Maintenance	
YSA04C: Sensitive Access – Client Admin		SE14		Utilities for Dictionary Tables	
YSA04D: Sensitive Access – Configuration Actions		SE37		ABAP Function Modules	
YSA04A: Sensitive Access – ABAP Admin		YSA04B: Sensitive Access – Archiving Admin	YSA04C	OY24	Client Administration
				OY25	Client Administration
				SCC4	Client Administration
				SCC5	Delete Client
SM30		Call View Maintenance			
SM31		Call View Maintenance Like SM30			
RZ10		Maintain Profile Parameters			
SM49		Execute External OS Commands			
YSA04D		YSA04D	SM50	Work Process Overview	

Firefighter Session Review

We will discuss:

- Automated Firefighter Session Review
- Design Decisions we made
- Overview of the future-state process
- Firefighter Access Remediation



Overview of GRC Firefighter Session Review



Replaced our legacy tool which was used to support the firefighter session review (FFSR) process through manual upload of data and push out of workflow items on a monthly basis.

Our future state process leverages the standard firefighter activity log review workflow and distributes the review items for each Firefighter session.

Process Design Decisions



Design Decision

1

Default time-period for FFID assignment will be 3 Days (exceptions for NetWeaver, Security, and Project related FF IDs and team members)

2

Log of sessions with no activity will be created

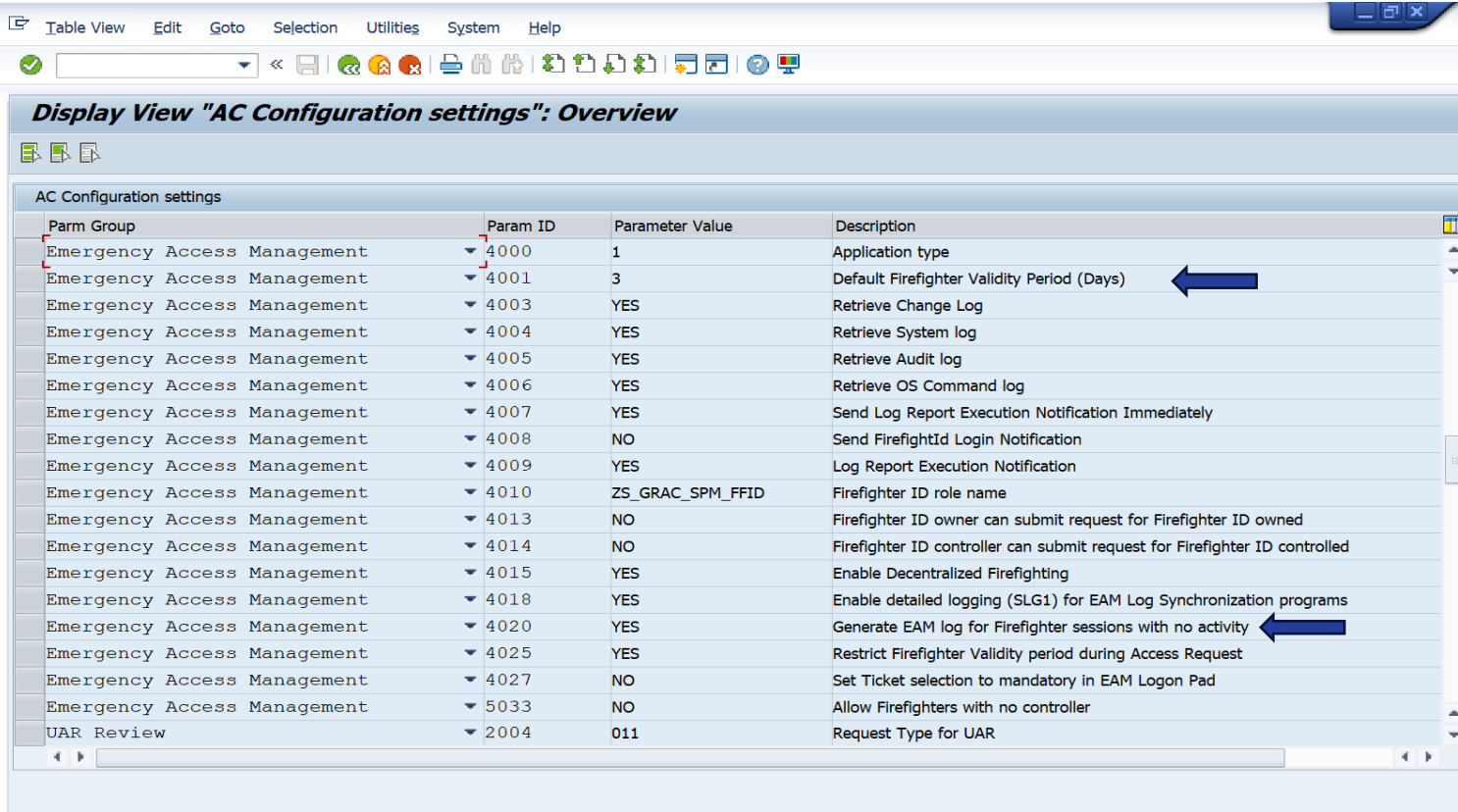
3

FF activity will be reviewed by session and sent immediately

4

FF log activity will be reviewed within 21 days by FFID controller

Access Control Configuration For Process Design Decisions





The screenshot displays the SAP IMG configuration settings for Emergency Access Management. The table lists various parameters with their IDs, values, and descriptions. Two blue arrows point to specific rows: one to the row with Param ID 4001 (Default Firefighter Validity Period (Days)) and another to the row with Param ID 4020 (Generate EAM log for Firefighter sessions with no activity).

Param Group	Param ID	Parameter Value	Description
Emergency Access Management	4000	1	Application type
Emergency Access Management	4001	3	Default Firefighter Validity Period (Days)
Emergency Access Management	4003	YES	Retrieve Change Log
Emergency Access Management	4004	YES	Retrieve System log
Emergency Access Management	4005	YES	Retrieve Audit log
Emergency Access Management	4006	YES	Retrieve OS Command log
Emergency Access Management	4007	YES	Send Log Report Execution Notification Immediately
Emergency Access Management	4008	NO	Send FirefightId Login Notification
Emergency Access Management	4009	YES	Log Report Execution Notification
Emergency Access Management	4010	ZS_GRAC_SPM_FFID	Firefighter ID role name
Emergency Access Management	4013	NO	Firefighter ID owner can submit request for Firefighter ID owned
Emergency Access Management	4014	NO	Firefighter ID controller can submit request for Firefighter ID controlled
Emergency Access Management	4015	YES	Enable Decentralized Firefighting
Emergency Access Management	4018	YES	Enable detailed logging (SLG1) for EAM Log Synchronization programs
Emergency Access Management	4020	YES	Generate EAM log for Firefighter sessions with no activity
Emergency Access Management	4025	YES	Restrict Firefighter Validity period during Access Request
Emergency Access Management	4027	NO	Set Ticket selection to mandatory in EAM Logon Pad
Emergency Access Management	5033	NO	Allow Firefighters with no controller
UAR Review	2004	011	Request Type for UAR

IMG Configuration Path: GRC → Access Control → Maintain Configuration Settings

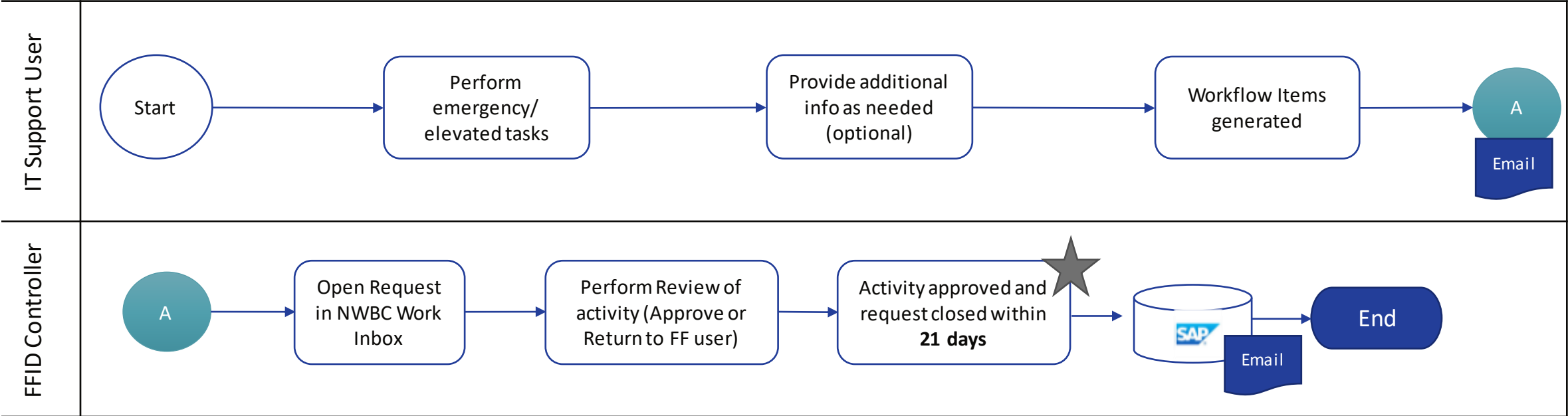
Participants in the FF Session Review Process

GRC includes the following participants that can appear in the Firefighter activity review process:

GRC Role	Description of Responsibilities	Jabil Resource Responsibility
 IT Support User	User that will perform emergency tasks requiring elevated access to critical transactions.	IT Support Team
 FFID Controller	Approvers at the Reviewer stage. The controller of a Firefighter ID, as defined in GRC.	Key IT Support Team Members by Functional Area

Firefighter Session Review Process Flow

This is a standard workflow-based review process within Access Control.
 The workflow item is sent to FF ID Controllers for review of activity for each FF ID session.



Key Firefighter Process Changes




Major pain point: high volume of activity in Firefighter IDs and lack of enough display access for IT display users

How we addressed this:

- Used analytics and dashboard to identify non-critical t-codes being executed with Firefighter IDs
- Reduce unneeded Firefighter logins in order to reduce volume of logs requiring review
- Moved closer to best practice processes for Firefighter usage and review by:
 - Performing continuous reviews based on sessions and not a monthly manual
 - Assignment of Firefighter IDs shortened to 3-day period for most IT support users, rather than long-standing access
 - **Note:** Exceptions were identified for specific IT support teams to have FF ID assignments for longer than 3 days

Firefighter Usage Analytics



Firefighter Usage Dashboard 2022

DATA UPDATED AS OF 10/31/22

System
PRD

Owner
All

Controller
All

Firefighter ID
All

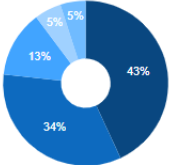
Total FFIDs

178

FF Session Usage
Total

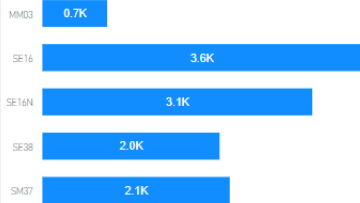
24K

Most Used Reason Codes
TOP 5 BY SESSION

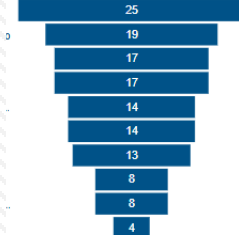


- PRODUCT REQUEST
- INCIDENT MANAG...
- SERVICE REQUEST
- BUSINESS USER
- REVIEW LOGS


Most Used Transactions
TOP 5



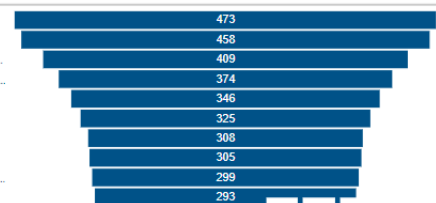
FFIDs per Owner
TOP 10



FF Sessions Executed per Month



Sessions Executed per Firefighter User
TOP 10



Firefighter ID	System	Firefighter	Date	Reason Code	Owner	Reason code description	Activity Description
FF_ARCHIVE	PRD		Monday, January 17, 2022	BU - BUSINESS USER		DB02 Statistics	DB02 space statistics check
FF_ARCHIVE	PRD		Thursday, January 27, 2022	BU - BUSINESS USER		Archiving	SARA
FF_ARCHIVE	PRD		Friday, January 28, 2022	BU - BUSINESS USER		Archiving	SARA
FF_ARCHIVE	PRD		Saturday, January 29, 2022	BU - BUSINESS USER		Archiving	SARA
FF_ARCHIVE	PRD		Monday, January 31, 2022	BU - BUSINESS USER		Archiving	SARA
FF_ARCHIVE	PRD		Tuesday, February 01, 2022	BU - BUSINESS USER		Archiving	SARA

- Developed PowerBI Dashboard based on standard Access Control report data.
- Leveraged dashboard to identify heavy users and log reviewers.
- Analyzed frequency of Firefighter ID use.
- Reviewed the most used t-codes with FF Controllers and FF Owners and identified display access activity which could be evaluated for assignment to standard user access.

Firefighter Access Remediation

High Level Outline of Firefighter Remediation Access Updates

1. **Update and improve communication** to FF ID owners on policy and standards for Firefighter ID use:
 - Re-educate and communicate updated FF ID Usage Standards (e.g., displaying data, mass update t-codes, etc.).
2. **Review current Firefighter ID assignments** and remove / reduce unneeded Firefighter IDs and access.
3. **Review SE16 access and provide display role** within Access Control for request by IT end users.
 - a. Role Owner will review requests and approve/reject based on appropriateness.
4. **Review roles with background job access** (SM37) and assign to end users to manage and monitor jobs (without administrator authorizations).



Firefighter Access Remediation (cont.)

High Level Outline of Firefighter Remediation Access Updates

5. **Review Mass Update T-codes:** SARA, LSMW, MASS, MASSD, MEMASSPO
 - Refer to SAP note 1378276 - The large amount of data associated with mass transaction/maintenance may cause the log collector job to run beyond the next scheduled job start.
6. **Considered creation of queries (SQVI)** for common data views and requests.
7. **Assign other display access for IT users** with required trainings. These roles do not contain any High or Critical transactions and have transactions codes commonly used within Firefighter IDs and were assigned to end users directly:
 - IT – ABAP Display
 - IT – ABAP Error Display
 - IT – Application Log Display
 - IT – EDI Display
 - IT – Workflow Display



Measuring Success with KPIs

In this section we'll cover some of the KPIs we used to monitor progress and measure success for reporting to our leadership team.





KPIs – Overall and UAR

	Area	Metric	Frequency	Baseline	Target	Measure
1	Overall	Count of SOX systems connected to GRC for automated UAR	One-time	0	6	Systems
2	UAR	Total number of days to perform and close user access review (UAR)	Annually	45	28	Days
3	UAR	Workload for the compliance team to prep and support user access review (UAR) process	Annually	450	50	Hours
4	UAR	Total number of days to perform user access review (UAR) by reviewer	Quarterly	30	14	Days
5	UAR	Completion percentage of access review	Annually	90%	95%	Roles



KPIs – Critical Transaction Access Review (CTAR)

	Metric	Frequency	Baseline	Target	Measure
1	Workload for the compliance team to prep and support for critical transaction review (CTR)	Quarterly	50	10	Hours
2	Number of risk owners assigned SoD risks. (target all risks have owners)	Annually	0%	100%	All BPOs
3	Total number of end users with critical sensitive access assigned.	Continuous	209	12	Users
4	Identification of user with critical risks versus high risks	Continuous	0	100%	Users
5	Number of critical t-codes monitored	Continuous	43	63	Tcodes



KPIs – Firefighter Metrics

	Metric	Frequency	Baseline	Target	Measure
1	Total number of days to perform FF activity log review (FFID Session Review)	Monthly	60	30	Days
2	Workload for the SAP governance team to prep support for FF activity log review (FFID Activity Review)	Monthly	Unknown	5	Hours
3	Total number of Firefighter activity logs reviewed according to security policy standards.	Monthly	100%	100%	Logs
4	Average number of end users assigned to Firefighter account.	Annually	900	250	Users
5	Total number of FF IDs	Continuous	525	300	FF IDs
6	Average number of FF sessions requiring review	Monthly	5.8K	3K	FF Sessions
7	Average number of days FF ID is assigned to a user (excluding Security and Basis)	Continuous	Unlimited	3	Days

Success in Numbers

35,000+
users



~90% of users reviewed within 35 days by Managers

1,000,000+
SAP access
assignments reviewed



Improved
precision of
critical access
monitoring

50%
reduction in
Firefighter
Assignments

**SAP Access
Governance
(GRC)**

User Access Review

Firefighter Activity Review

Critical Access Review

Critical Transaction
Execution Review

~200 hours
saved annually
supporting access
review tasks



4 new
automated workflows



Increased frequency of firefighter activity
review to daily



6 in scope systems



Wrap Up

- Understand control requirements and align GRC design decisions to ensure alignment with control objectives.
- Documenting completeness and accuracy takes time and a requires a good understanding of GRC tables and dependencies.
- Allocate sufficient time to testing and validating data.
- Measure success along the way to ensure effective communication to your leadership team.
- Automation is handled by GRC, but validation still requires some manual tasks!

Where to Find More Information

User Access Review (UAR) Reference Guide – SAP Access Control 12.0; SAP Help Documentation

https://help.sap.com/doc/4374b09eddfc468cb80b77b4ad83e80b/latest/en-US/AC12_UAR_Reference_Guide%20SP00.pdf

Troubleshooting UAR Request Generation; this page is to explain how to troubleshoot the UAR request Generation task; SAP Help Documentation

https://help.sap.com/docs/SUPPORT_CONTENT/grc/3362386995.html

SAP Access Management Governance – Getting it Right, Making it Sustainable; Protiviti

<https://www.protiviti.com/sites/default/files/2022-09/sap-access-mgmt-governance-getting-it-right-protiviti.pdf>

Achieve Seamless, Efficient SAP GRC Access Control Operations through Managed Services; Protiviti SAP Blog

<https://sapblog.protiviti.com/2022/08/02/achieve-seamless-efficient-sap-grc-access-control-operations-through-managed-services/>

Key Points to Take Home

- Evaluate standard Access Control functionality and design processes to support automated access review, risk review, and Firefighter activity review
- Leverage analytics to use data to provide insight into process and access issues
- Configure the system based on key design decisions and aligned to control objectives
- Leverage the ruleset to monitor and review sensitive access risks
- Understanding GRC functionality, table data, dependencies and aligning all of that with controls requires a cross-functional team and a good partner!



Thank you! Any Questions?



Susan Zortea

Susan_Zortea@jabil.com

[LinkedIn.com/in/susan-zortea-94187811/](https://www.linkedin.com/in/susan-zortea-94187811/)



Hannah Sears

Hannah_Sears@jabil.com

[LinkedIn.com/in/hannah-sears-27b7581b0/](https://www.linkedin.com/in/hannah-sears-27b7581b0/)

Please remember to complete
your session evaluation.



SAPinsider.org

PO Box 982 Hampstead, NH 03841
Copyright © 2024 Wellesley Information Services.
All rights reserved.

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. Wellesley Information Services is neither owned nor controlled by SAP SE.

**SAPinsider
comprises the
largest and fastest
growing SAP
membership group
with more than
800,000 members
worldwide.**
