



Conference Essentials: Understanding the basics of SAP S/4 HANA Application and Cyber Security, Access, Process Control and Identity and Access Governance (IAG)

Ray Mastre, Accenture LLP

SAPinsider
Las Vegas

2023

SAPinsider

About the speaker

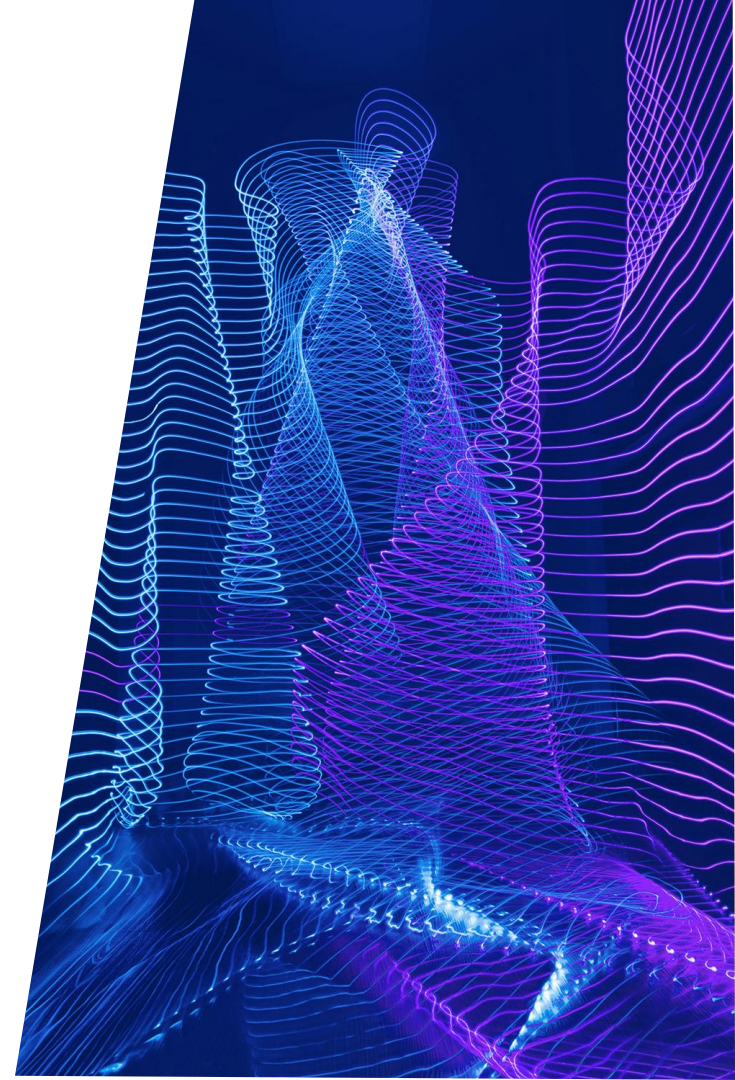


~19 years

of SAP Security / SAP GRC / SAP
Controls experience

17 years

in Big 4 consulting

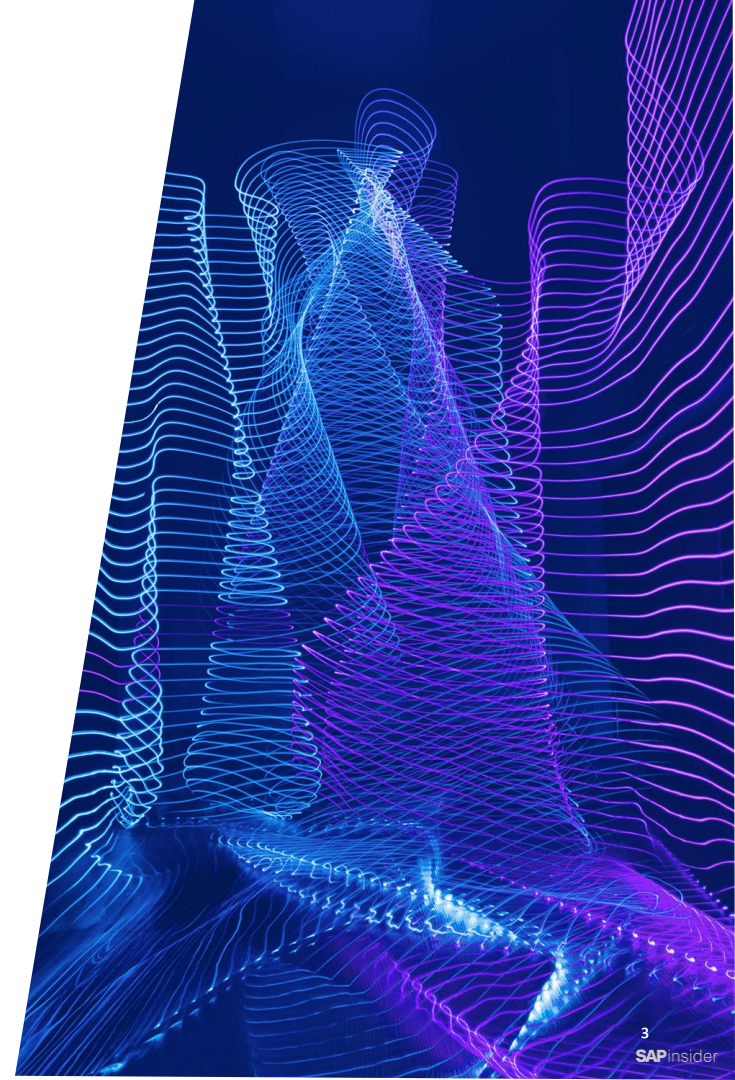


Attendee Poll (1 of 4)



**What role do you play in
your organization?**

- SAP Security / SAP Access Control (AC) Admin
- SAP Basis / Developer / Other SAP Technical
- Internal Audit
- Business / Finance
- Other

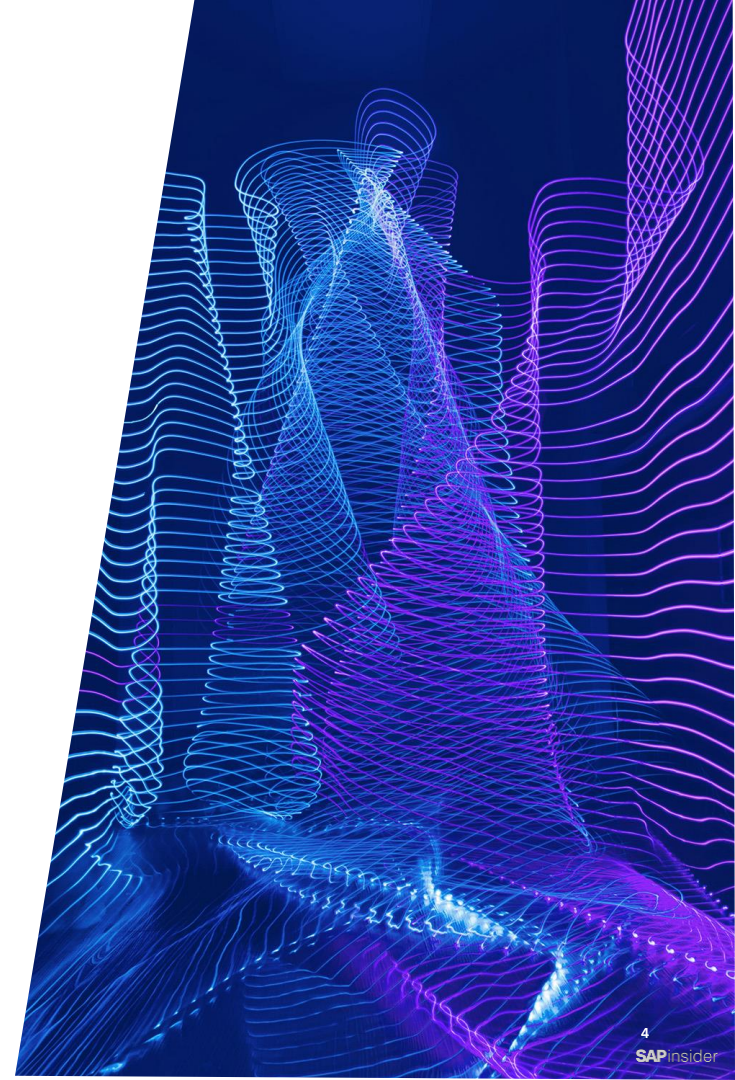


Attendee Poll (2 of 4)



**Where is your organization
on its S/4 journey?**

- Already on S/4 HANA
- CFIN or other preliminary stage
- S/4 project is in process
- Starting in 6 months
- Starting in 12+ months
- I don't know

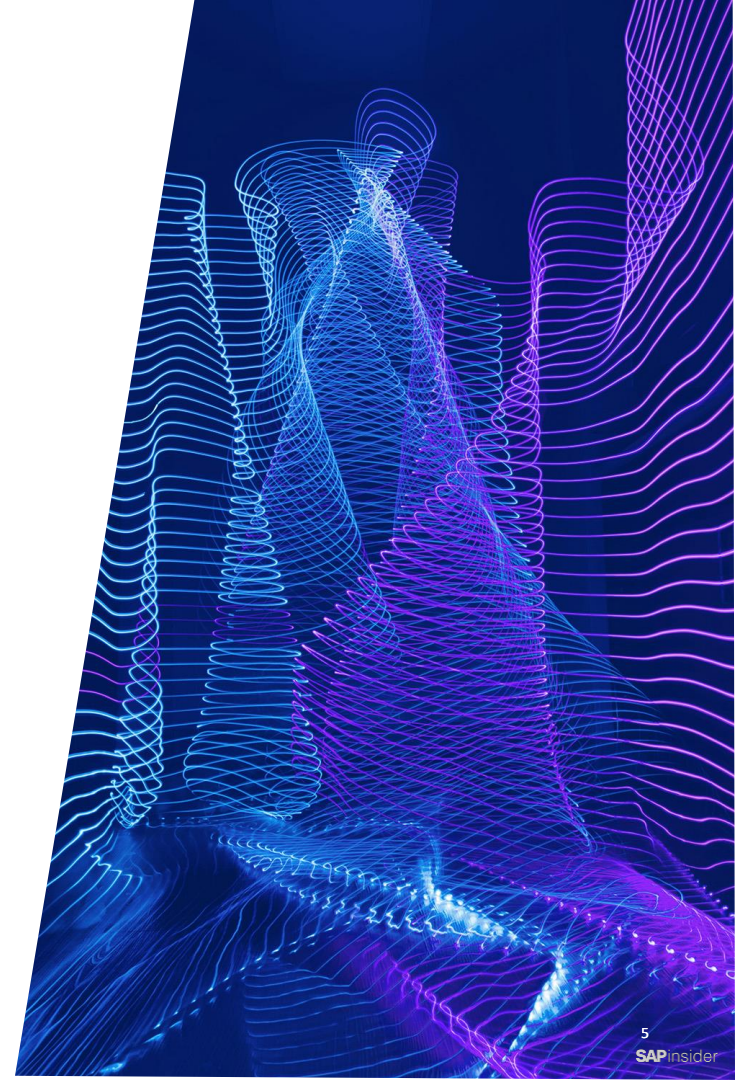


Attendee Poll (3 of 4)



How aware are you of SAP Cyber Security threats?

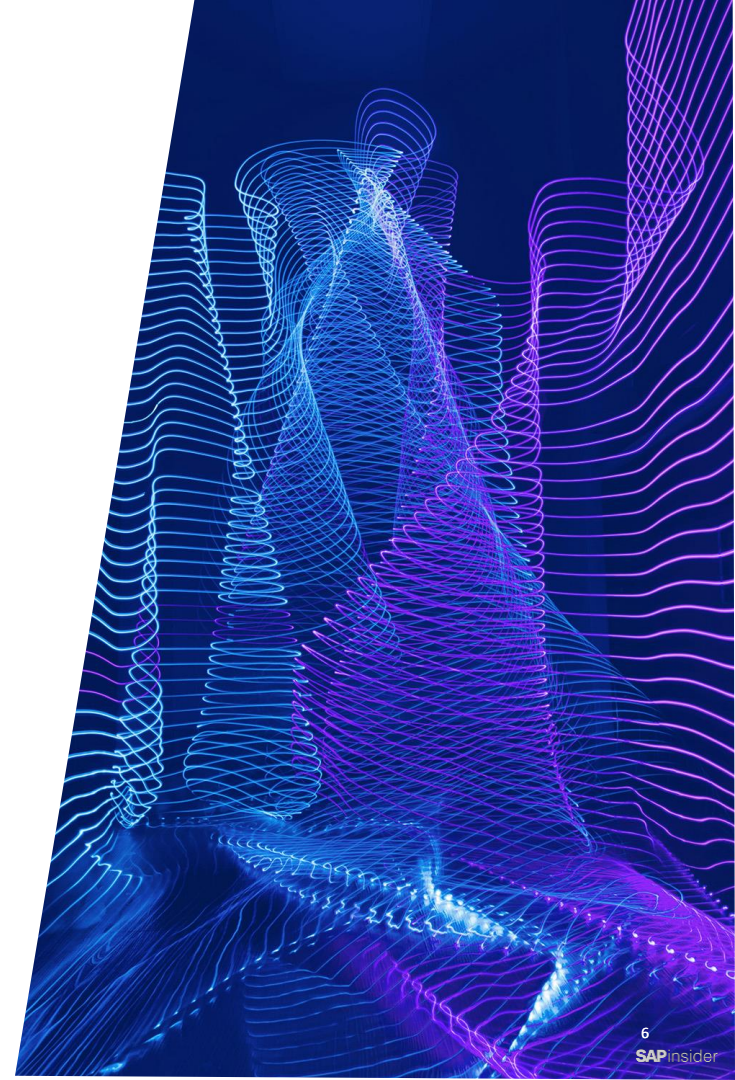
- I'm a pro – bring on the threat actors!
- I know enough to be dangerous
- I don't know much – teach me!



Attendee Poll (4 of 4)



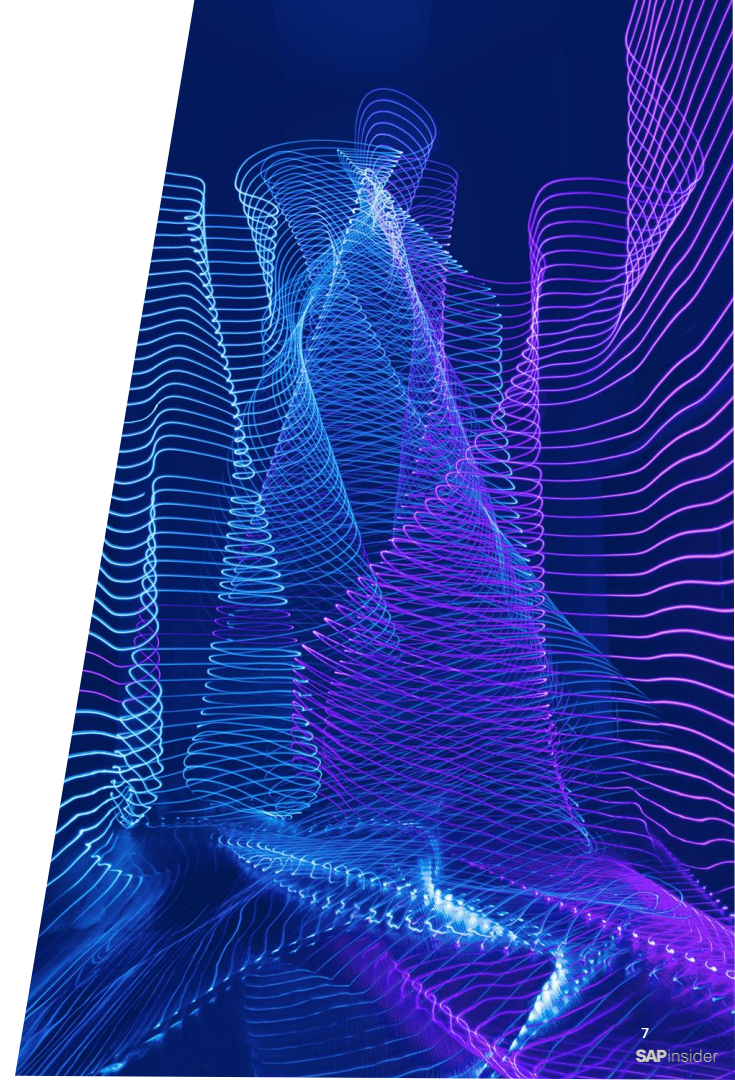
**What do you hope to get out
of this presentation?**



Goal of this session



The goal of the conference essentials session is to prepare you for the conference by providing a base knowledge on SAP Security, SAP AC/PC and SAP Cyber Security to allow you to dive deeper in future conference sessions.



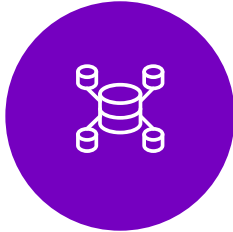
What we'll cover

- **SAP Security and GRC – Why important?**
- **Introduction to SAP Security**
 - How security works in SAP
 - Differences between SAP ECC and S/4 HANA
 - Key design methodologies
 - Security key performance indicators / governance
- **Introduction to SAP GRC**
 - SAP Access Control (AC)
 - SAP Identity and Access Governance (IAG)
 - SAP Process Control (PC)
- **Introduction to SAP Cyber Security**
- **Wrap up**



SAP Security – Why important?

Why is securing your SAP environment so important?



Security is the gateway to your SAP system.



SAP system contains some of the most valuable information of the company.



SoX and other compliance related requirements (ITAR, HIPAA, GxP, etc.)

Impacts of poor security

Some of the impacts of poor SAP Security are as follows...what else have you seen?



Inefficiencies due
to access issues



Financial
misstatement



User error



Sox issues



Reputational
damage



Loss of
critical data



Financial loss

Components of successful SAP Security programs

Best run security programs incorporate three components on top of a known list of critical assets.



Security roles



Provisioning
technology



Optimized
processes

Critical asset inventory

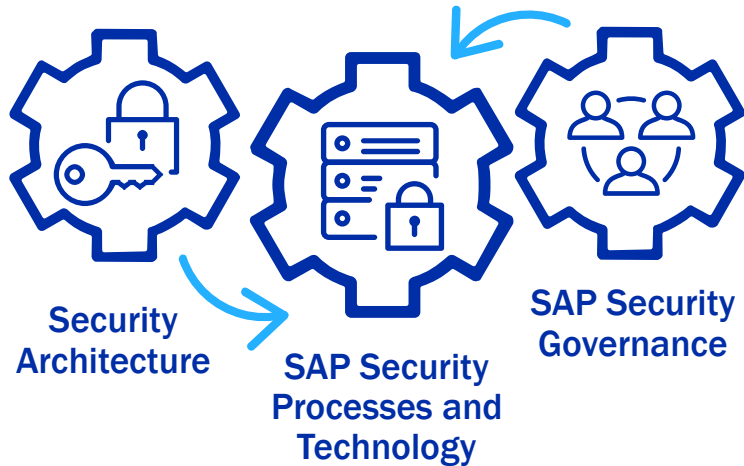
What we'll cover

- SAP Security and GRC – Why important?
- **Introduction to SAP Security**
 - How security works in SAP
 - Differences between SAP ECC and S/4 HANA
 - Key design methodologies
 - Security key performance indicators / governance
- **Introduction to SAP GRC**
 - SAP Access Control (AC)
 - SAP Identity and Access Governance (IAG)
 - SAP Process Control (PC)
- **Introduction to SAP Cyber Security**
- **Wrap up**



What is SAP Security?

“SAP Security” is not just technical. It is made up of three main components:



- Focusing only on architecture can lead to faulty security via processes and governance
- Business governance is typically the hardest of the three areas to achieve success

Major security changes in S/4 HANA

There are two major differences between SAP ECC and S/4 HANA Security:



01

Increased
database
access

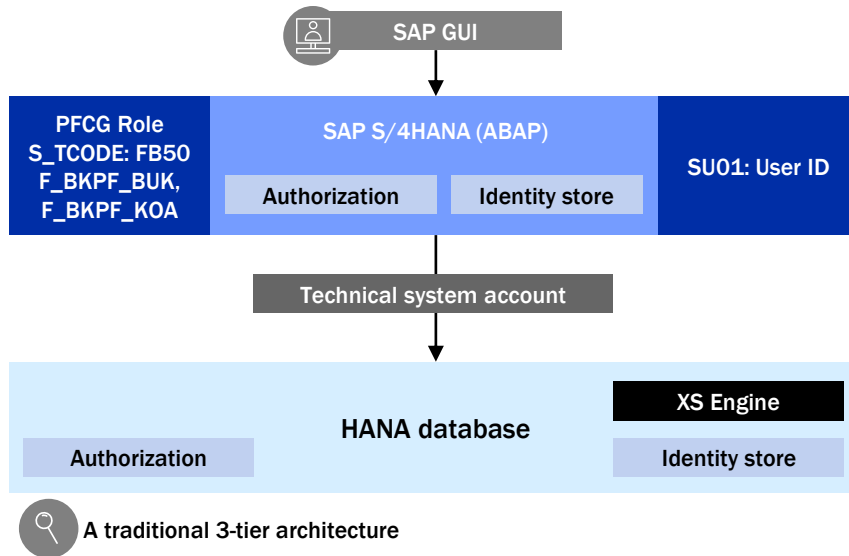


02

Access to
the Fiori
Gateway

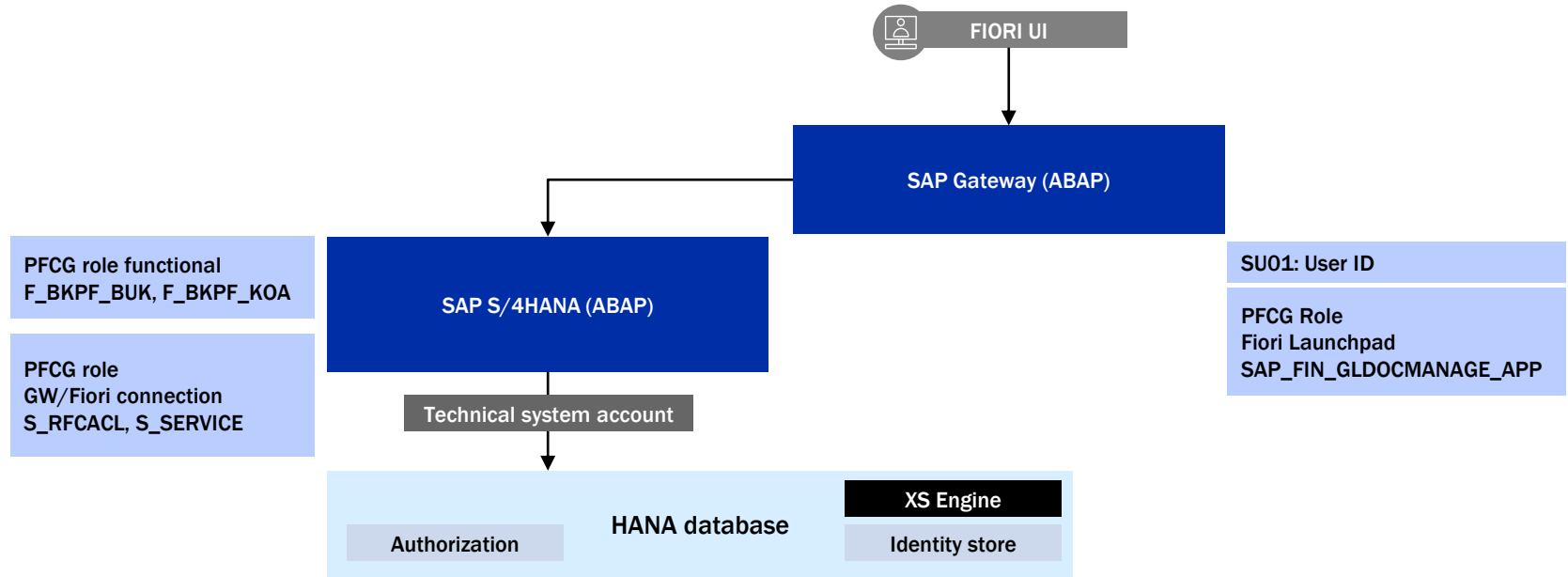
Case study #1: SAP GUI – FB50 Transaction

Traditional ways of accessing SAP still exist in S/4 HANA:



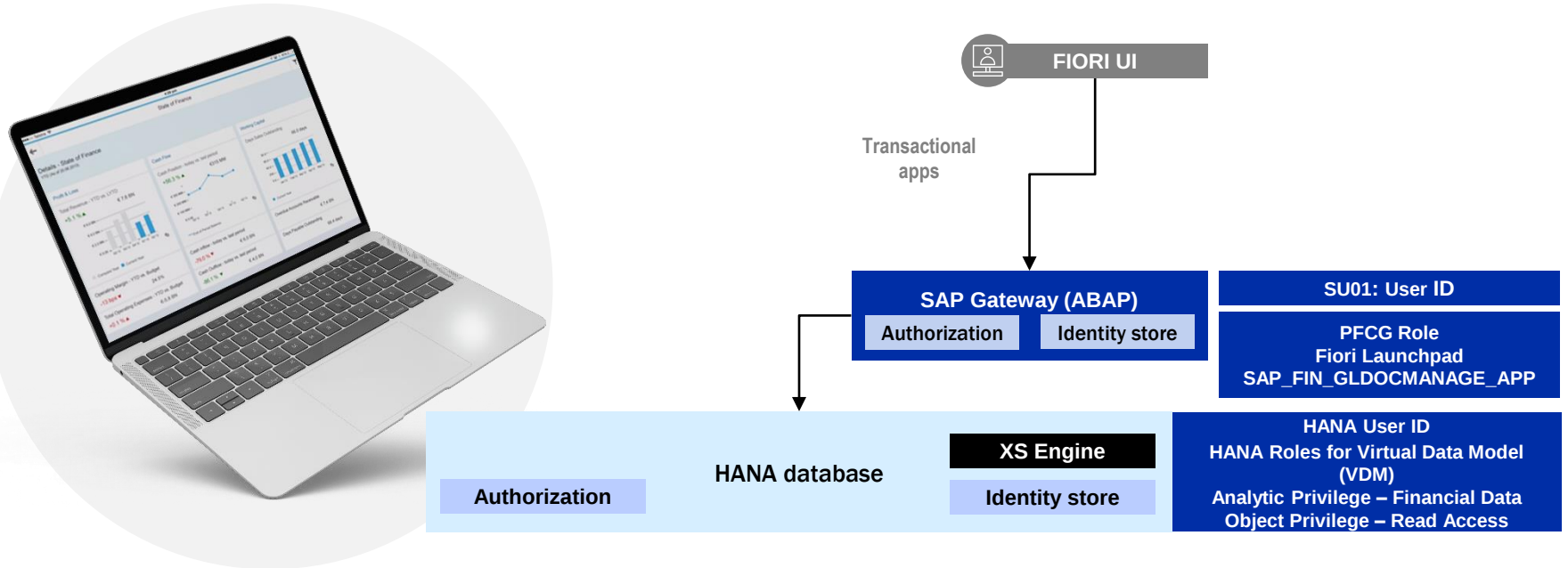
Case study #2: Fiori – Post financial document

Most Fiori applications do NOT require a HANA ID:



Case study #3: Fiori analytic – Closing dashboard

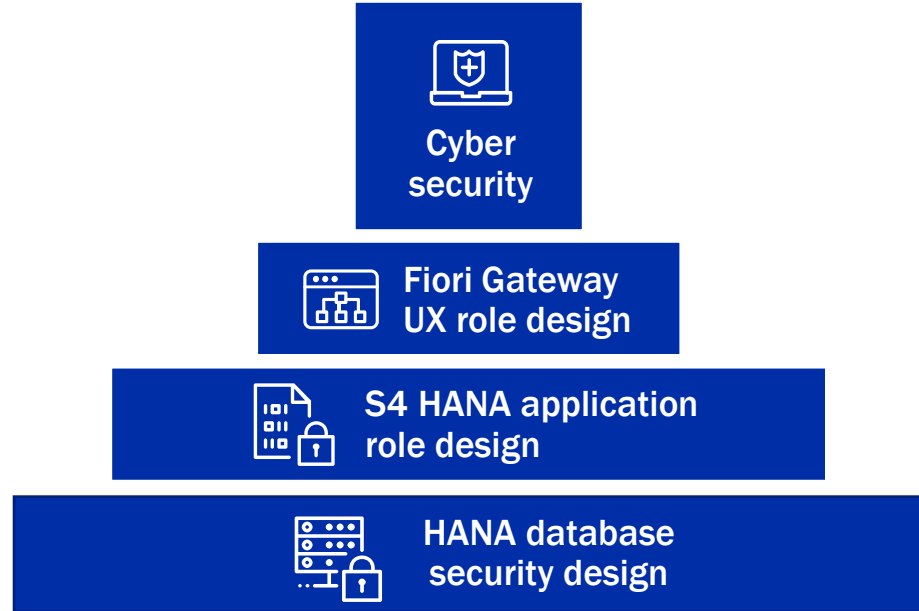
Analytic applications require an ID in HANA:



More than just application layer



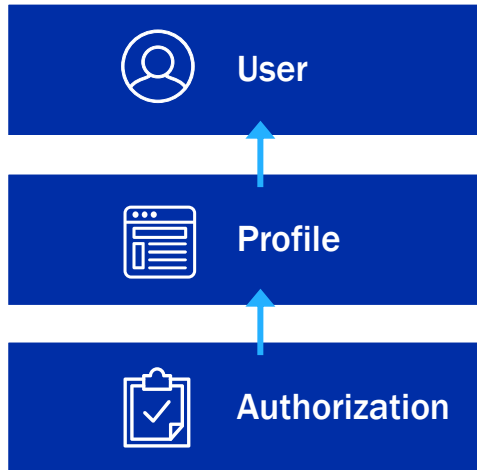
Security teams can no longer worry about just application-level security.



Basics of S/4 Security



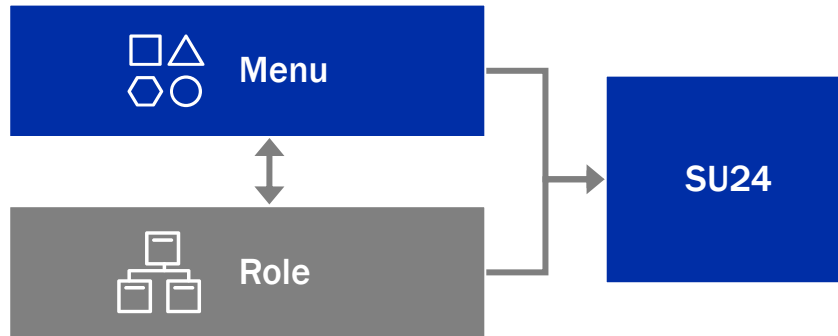
SAP Authorization Structure



Basics of S/4 Security

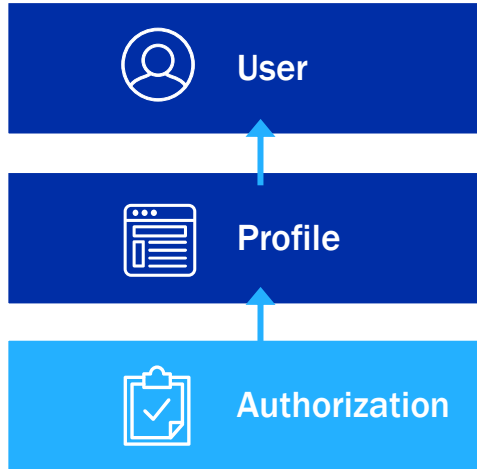


SAP Building Blocks

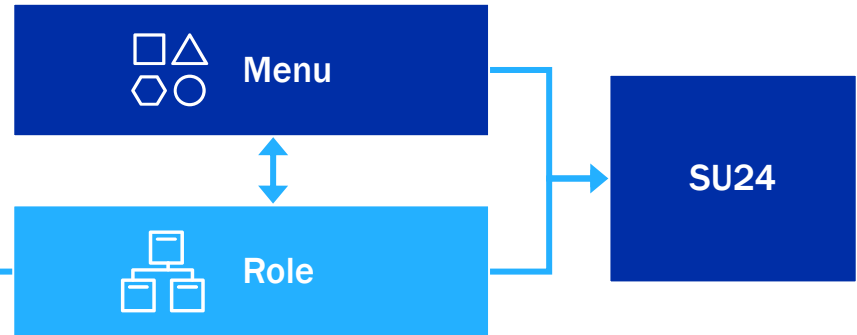


Basics of S/4 Security

SAP Authorization Structure



SAP Building Blocks



The Fiori Security approach

Business users will be given three types of SAP Fiori applications:



Transactional Applications: Access to activities like change, create or entire processes with guided navigation



Analytical Applications: Visual overview of a dedicated topic for further KPI (key performance indicator) related analysis



Fact Sheet Applications: View essential information about objects and contextual navigation between related objects

The Fiori Security approach

The following are the key steps which need to be implemented to enable security restrictions within the SAP Fiori applications:



Frontend server (Gateway System)

- UI PFCG roles for Fiori Launchpad (example – S_SERVICE) – contains assigned references to Fiori Launchpad catalog(s)



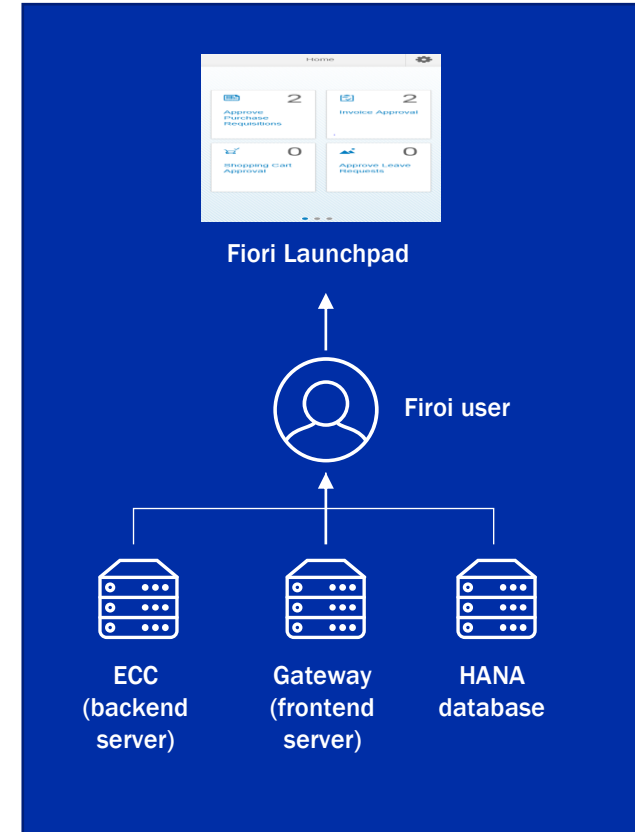
Backend server (ECC System)

- ODATA PFCG roles - contains assigned references to ODATA service SU22 entries
- RFC authorizations – S_RFCACL and S_RFC
- Business authorizations



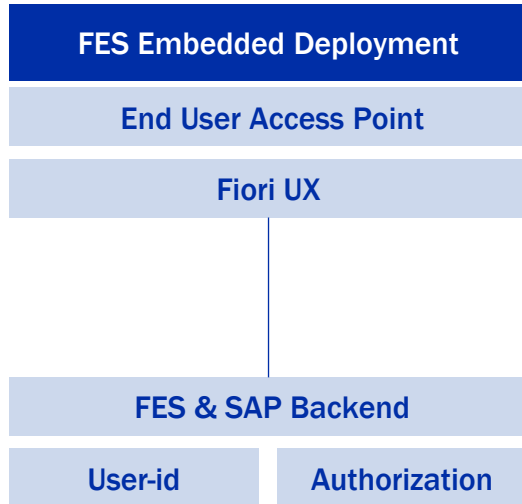
HANA database

- Privileges for analytical applications
- Test

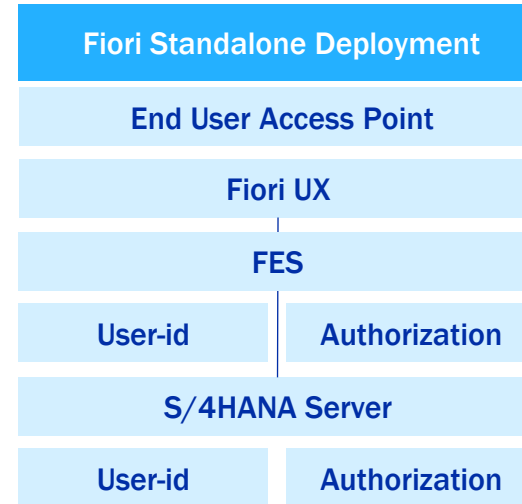


Fiori – Embedded vs. Standalone server

Embedded FES deployment is recommended for S/4HANA. The FES and SAP backend exist on the same server.



Standalone Server deployment is recommended for SAP Business Suite. The FES and SAP backend exist on different servers. This can connect to one or more backends.



Fiori – Adding standard Fiori App to role

Fiori security requirements are publicly available on the [Fiori app library](https://fioriappslibrary.hana.ondemand.com/sap/fix/externalViewer/)

The screenshot shows a web browser window with the URL `fioriappslibrary.hana.ondemand.com/sap/fix/externalViewer/`. The browser's address bar includes navigation icons (back, forward, refresh, home) and a lock icon. Below the address bar, there are links for 'Home' and 'MCK'. The main content area features a dark blue header with the SAP logo and a home icon. A sidebar on the left lists categories: 'All apps', 'All apps for SAP S/4HANA', 'SAP Fiori apps for SAP S/4HANA', and 'SAP Fiori apps for SAP Business Suite', each with a right-pointing arrow. The main content area displays a welcome message: 'Welcome to the SAP Fiori Apps Reference Library!' in blue text, followed by a paragraph: 'Explore, plan and implement SAP Fiori, the latest user experience from SAP inc launchpad.'

Categories	
All apps	>
All apps for SAP S/4HANA	>
SAP Fiori apps for SAP S/4HANA	>
SAP Fiori apps for SAP Business Suite	>

Welcome to the SAP Fiori Apps Reference Library!

Explore, plan and implement SAP Fiori, the latest user experience from SAP inc launchpad.

Fiori – Fiori app library Odata services

Go to FIORI APP LIBRARY in Chrome and search for the app: “Depreciation Lists “

Below is the ODATA service for this app:

The screenshot shows the SAP Fiori Apps Library interface. The search results for 'Depreciation Lists' are displayed. The app is identified as 'F1616' and is categorized under 'Other SAP Fiori Apps'. The app details include:

- App ID: F1616
- Required Back-End Product: SAP S/4HANA
- Line of Business: Finance
- Application Type: Transactional (SAP Fiori elements)
- Database: HANA DB exclusive
- Form Factor: Desktop, Tablet
- App ID: F1616

The app is titled 'Depreciation Lists' and is described as 'for Asset Accountant'.

The screenshot shows the 'App Details' page for the 'Depreciation Lists' app. The app is identified as 'F1616' and is categorized under 'Other SAP Fiori Apps'. The app details include:

- App ID: F1616
- Required Back-End Product: SAP S/4HANA
- Line of Business: Finance
- Application Type: Transactional (SAP Fiori elements)
- Database: HANA DB exclusive
- Form Factor: Desktop, Tablet
- App ID: F1616

The app is titled 'Depreciation Lists' and is described as 'for Asset Accountant'.

OData Service(s)

The following OData services must be activated on the front-end server
Users require PFCG authorization for the front-end and back-end systems.

OData Service	Version	Software Component Version	Back-End Authorization Role (PFCG)
FAA_ASSET_DEPRECIATION_LIST_SRV	0001	S4CORE 103	SAP_BR_AA_ACCOUNTANT

SAP Fiori Launchpad

You require the following data to give users access to the app in the SAP Fiori launchpad.

Technical Configuration

Technical Catalog	SAP_TC_FIN_ACC_COMMON

Fiori – Catalog and group from Fiori app library

Go to FIORI APP LIBRARY in Chrome and search for the app: “Depreciation Lists “

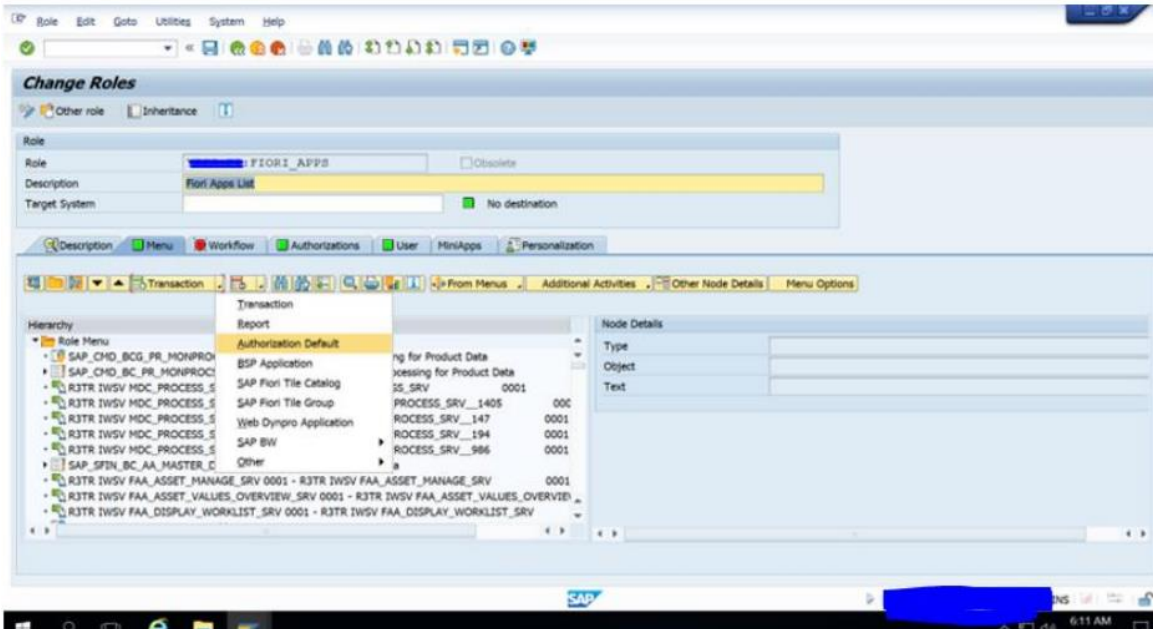
Below you can find the Group and Catalog information

Apps (1)		App Details	
F1616	⊗ 🔍		
Other SAP Fiori Apps			
☐ Depreciation Lists			
		Business Catalog(s) Extend Apps Selection	
		☐ Catalog Name	Catalog Description
		☐ SAP_SFİN_BC_AA_GEN_REP	Asset Accounting - General Reporting
		Business Group(s)	
		Business Group	Group Description
		SAP_SFİN_BCG_REPORTING	Reporting

**Basis will need to activate the ODATA and SICF services in SAP system

Fiori – Security requirements and catalog

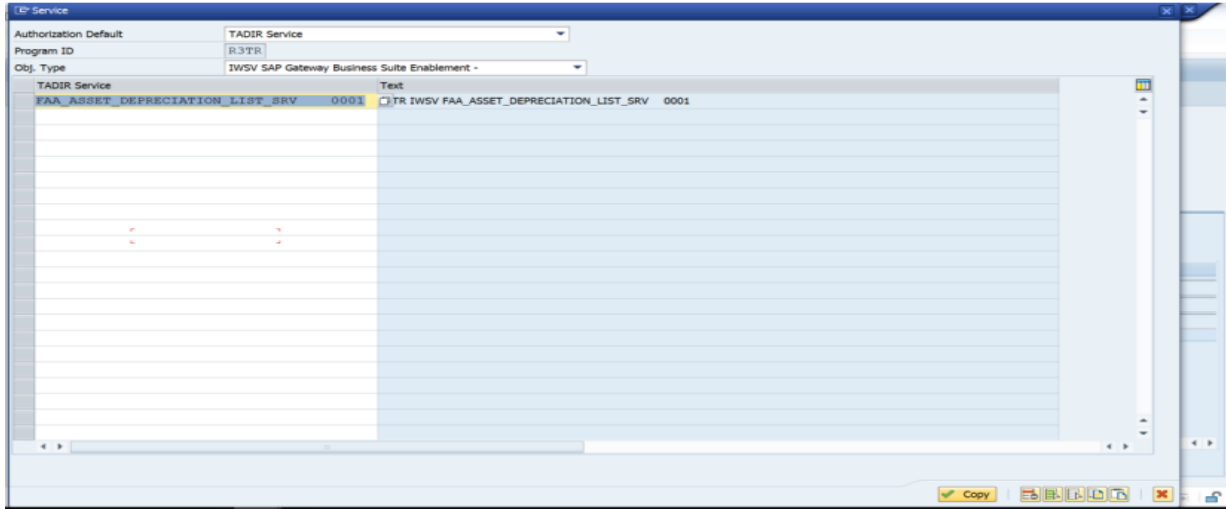
Adding ODATA Services To Role



Fiori – Adding Odata services to role

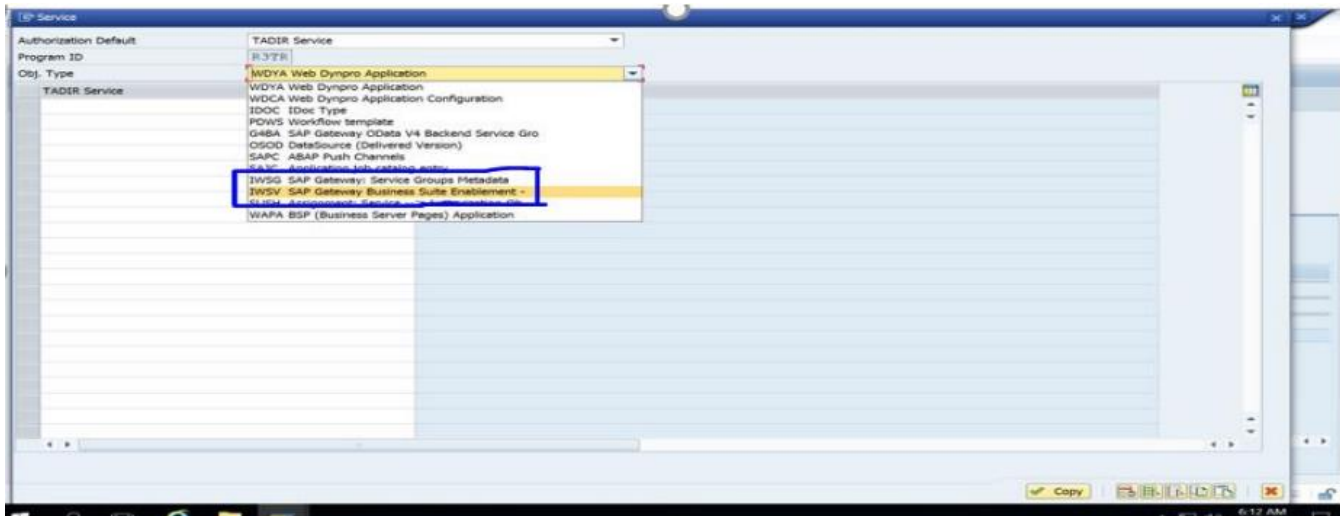
Enter the ODATA service name with prefix * and hit F4.
Select the checkbox with 0001 version and APPLY.

Click on copy below and the ODATA service will be added to the menu



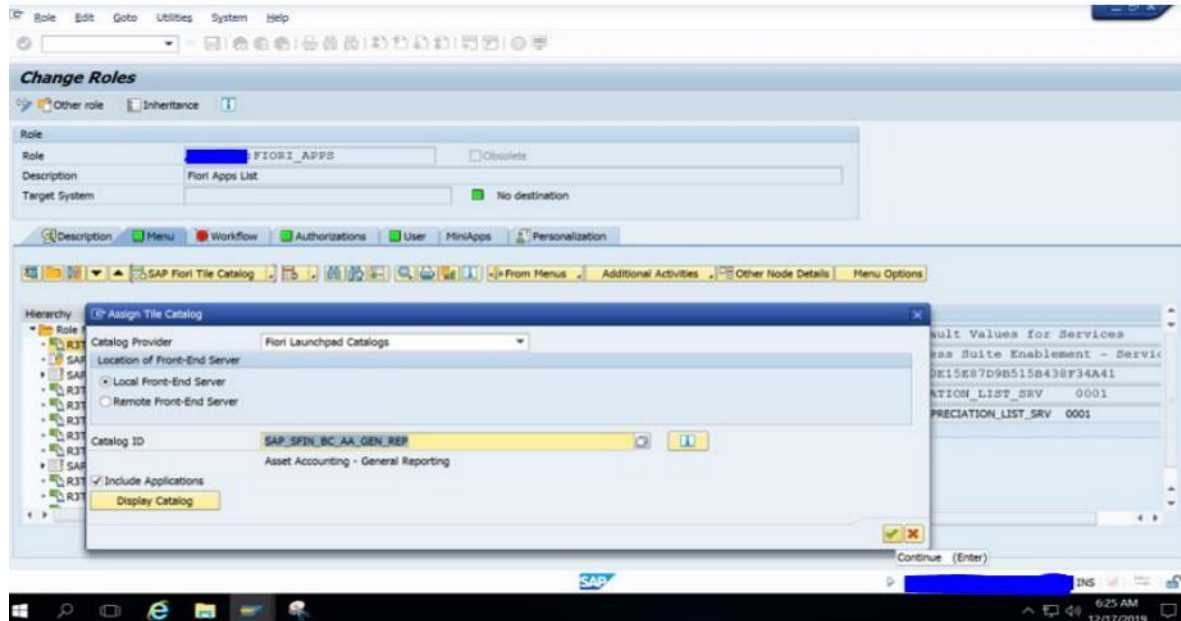
Fiori – Adding Odata services to role

We use IWSG and IWSV for adding ODATA services. IWSV is for backend and IWSG is for frontend Fiori Gateway. When we use Embedded Fiori setup, we use IWSG and IWSV in the same system, else we need to use IWSV in backend and IWSG in frontend system



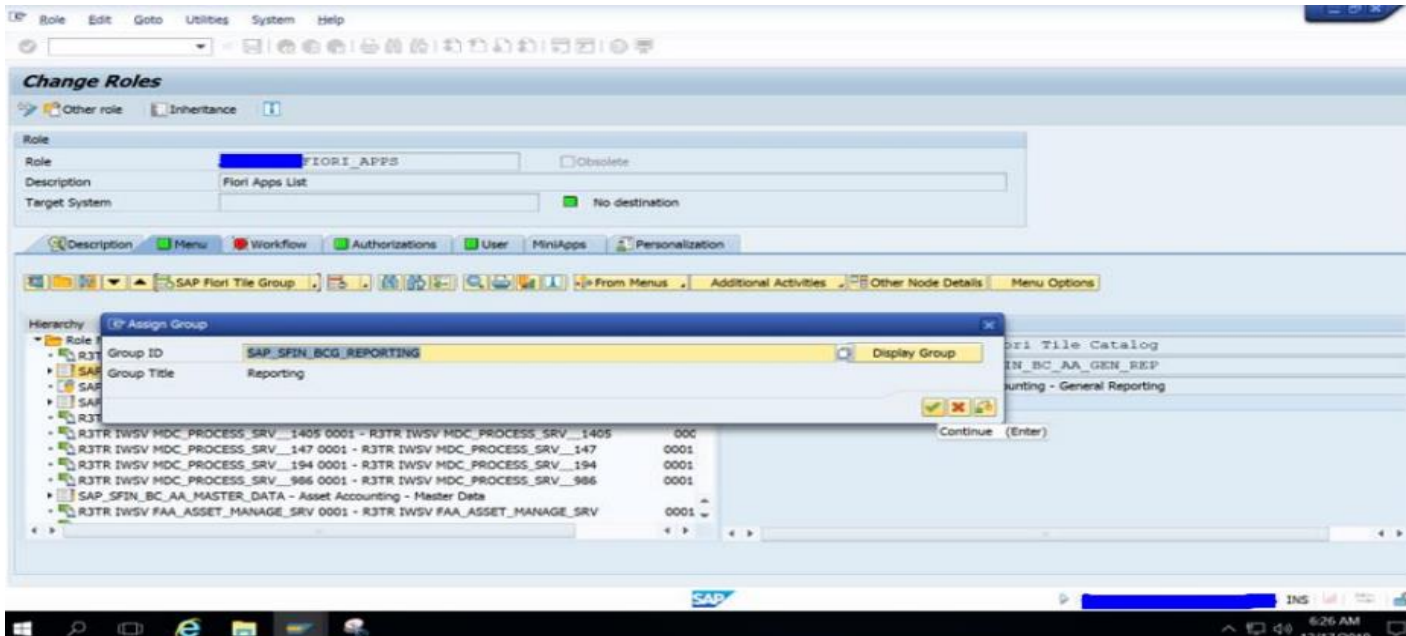
Fiori – Adding catalog to role

Enter the catalog we got from library with suffix * and hit F4. select SAP FIORI TILE CATALOG



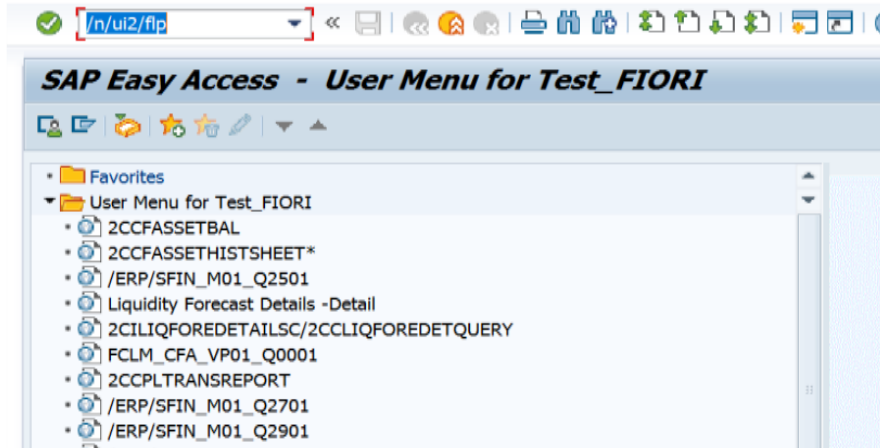
Fiori – Adding group to role

Select SAP FIORI TILE GROUP from dropdown as shown below



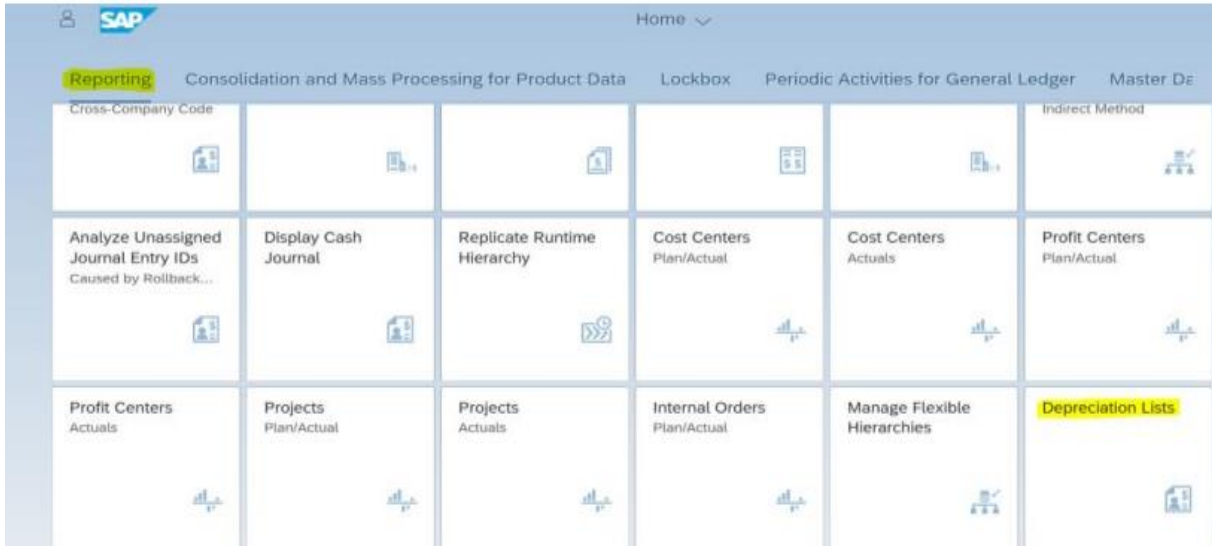
Fiori – Testing with user-id with the security role

Login with the test ID and password which is assigned to this role: Execute t-code /N/UI2/FLP:



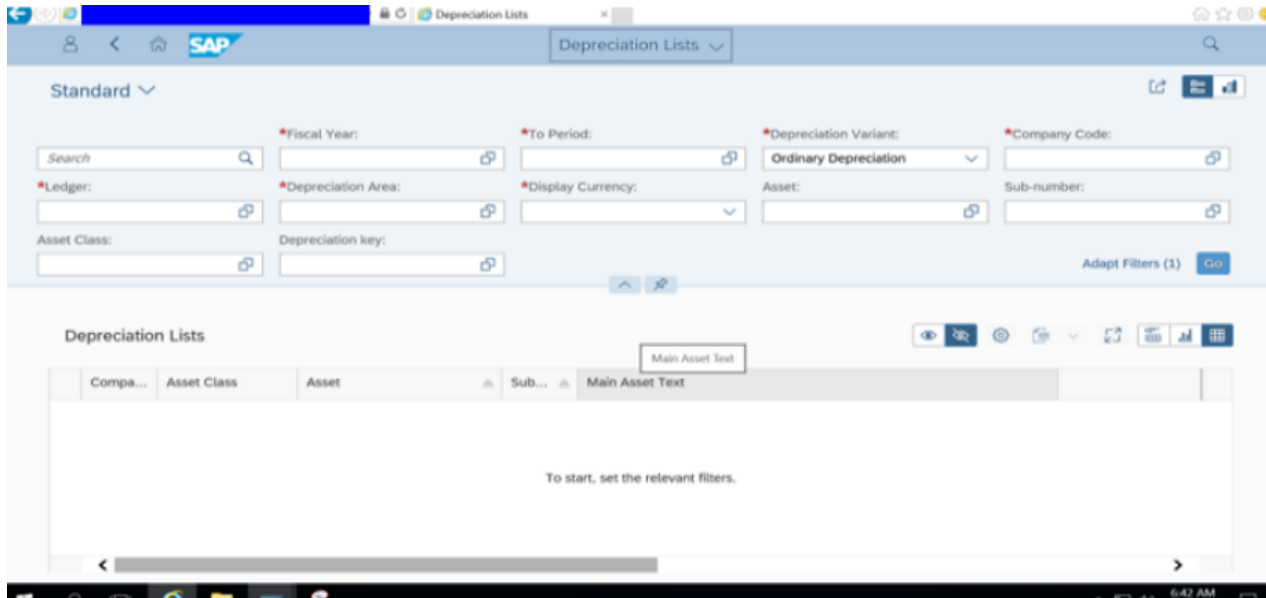
Fiori – Testing the Fiori app

You will be redirected to FIORI LAUNCHPAD as below: Reporting is the GROUP name, and “Depreciation List” is the tile catalog for app F1616.



Fiori – Testing the Fiori app

The app “depreciation lists” opens and we are able to see the screen below:



Security design methodology

1

Tier 1: General access

- Provisioned via one single role
- Non-critical transactions common to all users
- Includes items like: printing, inbox, SU53, etc.

2

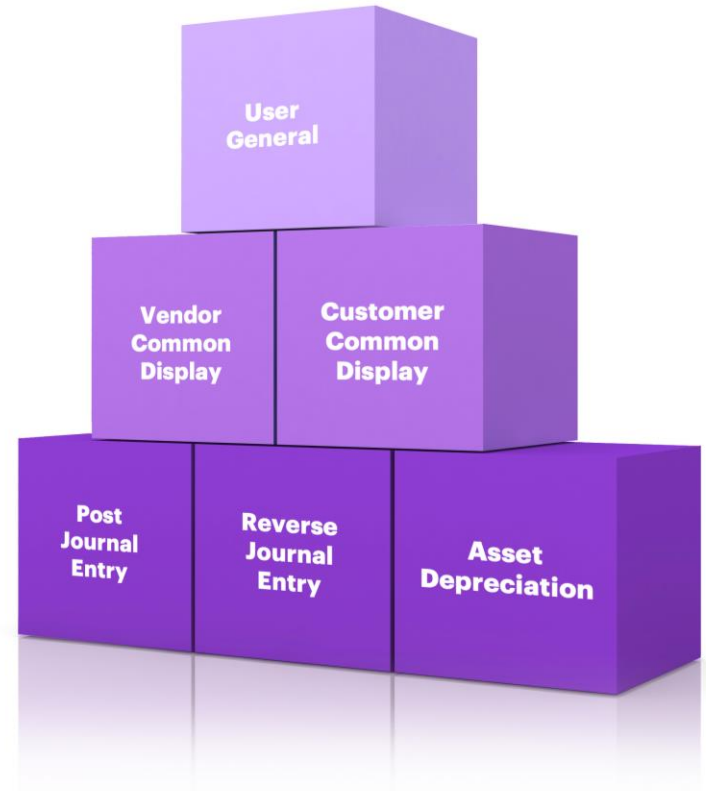
Tier 2: Display access

- Provisioned via a set of roles defined by functional area
- Allow display and reporting access intended to compliment the functional roles of a user

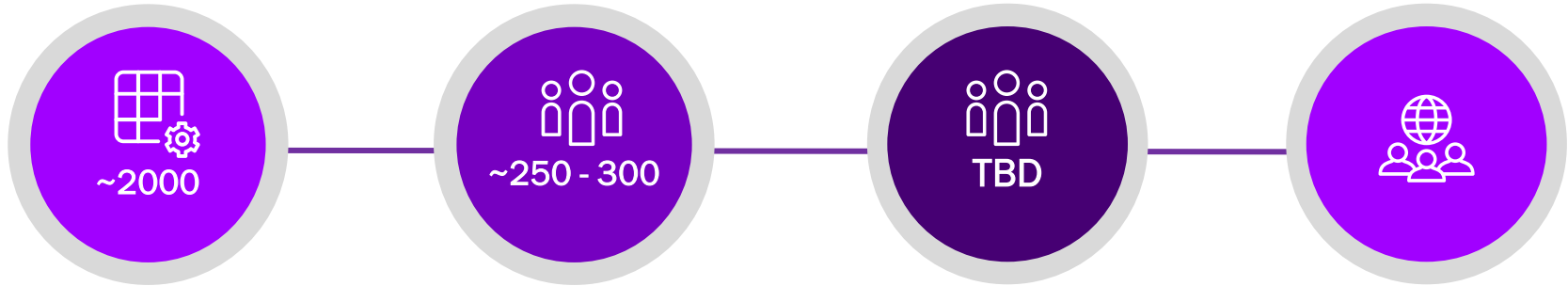
3

Tier 3: Functional access

- Privileges for analytical applications
- Test



Security design methodology



Transaction codes

- Transaction codes based on business requirements

Task roles

- Secured based on relevant control points.
- No duplicate transactions
- Free of SoD conflicts
- Building blocks for the job roles

Business unit job roles

- “Role of Roles” providing users access to do their job with relevant control points (ex. Account Payables Administrator, Inventory Manager, etc.)
- Based on the 3 tier security design methodology

Business users

- A user may have 2-3 job roles depending on the resource availability to perform the job.
- May have SoD conflicts but should be kept to a minimum of 1-2 SoDs.
- Controls should be developed and monitored to mitigate SoD conflicts

Security key performance indicators

How do you track the “success” of your SAP Security? Several companies have created Key Performance Indicators to track the health of their security.



Some metrics of success may include:

- # of transactions / apps in the security design
- # of roles with manual / change authorizations
- Intra-role SoD violations
- User-level SoD violations
- # of SAP users
- # of SAP roles
- Etc.
- Etc.

What we'll cover

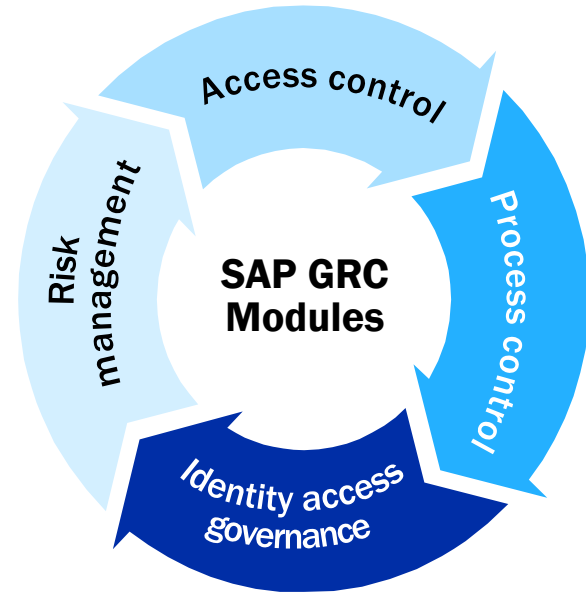
- SAP Security and GRC – Why important?
- Introduction to SAP Security
 - How security works in SAP
 - Differences between SAP ECC and S/4 HANA
 - Key design methodologies
 - Security key performance indicators / governance
- **Introduction to SAP GRC**
 - SAP Access Control (AC)
 - SAP Identity and Access Governance (IAG)
 - SAP Process Control (PC)
- Introduction to SAP Cyber Security
- Wrap up



SAP GRC Overview



SAP governance, risk and compliance (SAP GRC) is a powerful SAP security tool that can be used to ensure your company meets data security and authorization standards.



SAP GRC Overview

Access Control (AC)

- Access risk analysis (ARA)
- Access request management (ARM)
- Emergency access management (EAM)
- Business role management (BRM)



Process Control

- Risk and compliance document repository
- Manual and continuous control monitoring
- Issue and remediation management
- Compliance evaluation
- Policy and procedure management
- Reporting

Identity & Access Governance

Access control for cloud systems

SAP Access control components



Access risk
analysis



Business role
management



Access request
management



Emergency
access
management



User access
review

Access Risk Analysis (ARA)

ARA modules let you identify and detect access violations in the entire enterprise.



Features:

- Enables you to define access risks (via a rule set)
- Helps identify realized access risks (via risk analysis)
- Simulates and reports risk analysis on user and roles for potential risks
- Assigns and tracks mitigating controls

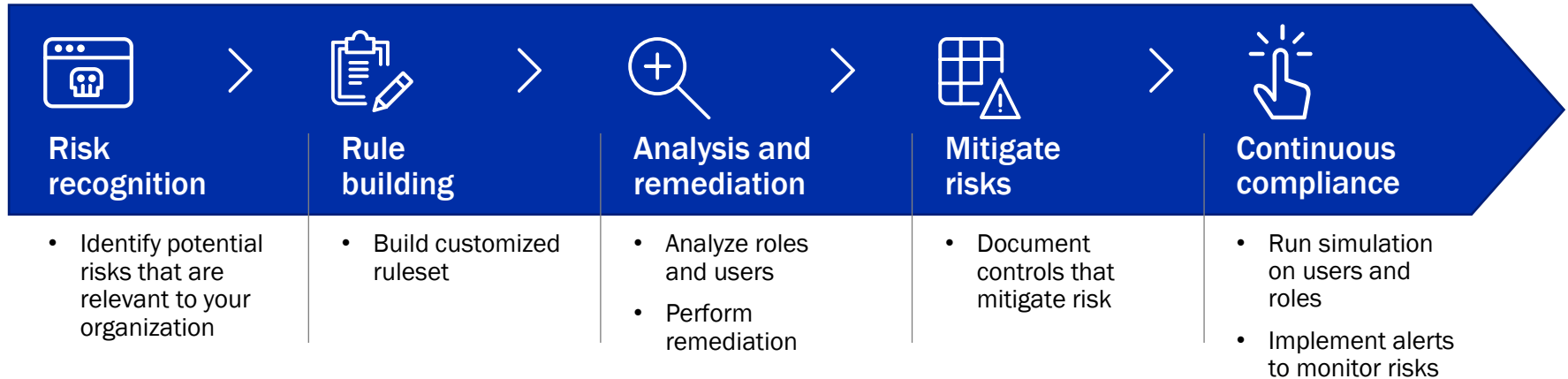


Benefits:

- Reporting risks at role and user level

Access Risk Analysis

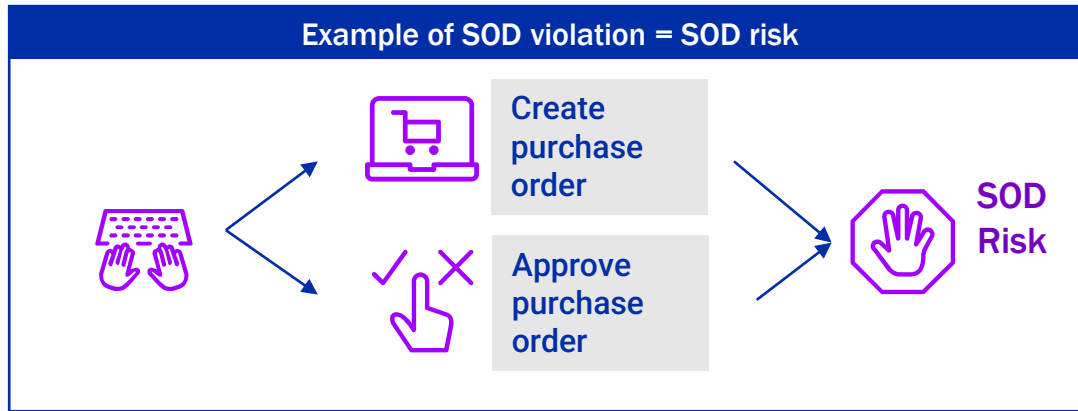
Building a SoD ruleset, typically follows this process:



Access Risk Analysis

Segregation of duties involves separating steps in a business process to prevent errors or fraud.

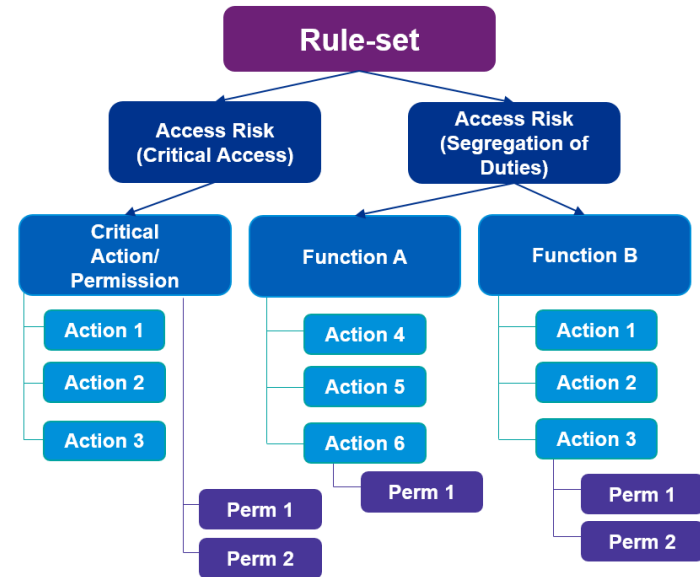
**No single individual/user role in the system has control over two or more phases of a transaction or operation that can lead to financial fraud.



Access Risk Analysis: SOD Ruleset

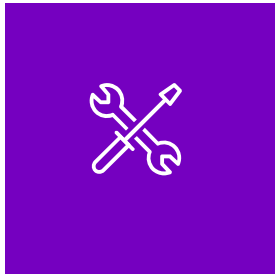
A ruleset is the basis for carrying out a risk analysis in the SAP system.

- A SOD risk is a set of conflicting business functions.
- A function is a set of actions that comprise a business function.
- Action and permission are the transaction and authorizations within.



Access Risk Analysis: Workflows

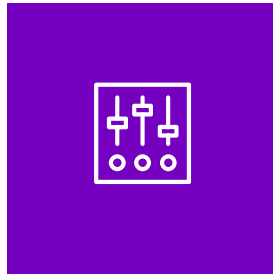
The following workflows may be configured to support ARA:



Risk
maintenance



Function
maintenance



Mitigation control
creation



Mitigation control
assignment



SOD/sensitive
access reviews

Emergency Access Management (EAM)

EAM manages access of superusers when troubleshooting unplanned IT emergencies.



Features:

- Provides centralized access and administration of firefighter IDs
- Enables event-based logging for emergency access sessions
- Detailed audit trail of performed actions and web-based reporting
- Integrates with access request management module to support log review workflow and drives accountability and audit ability in the firefighter log review process



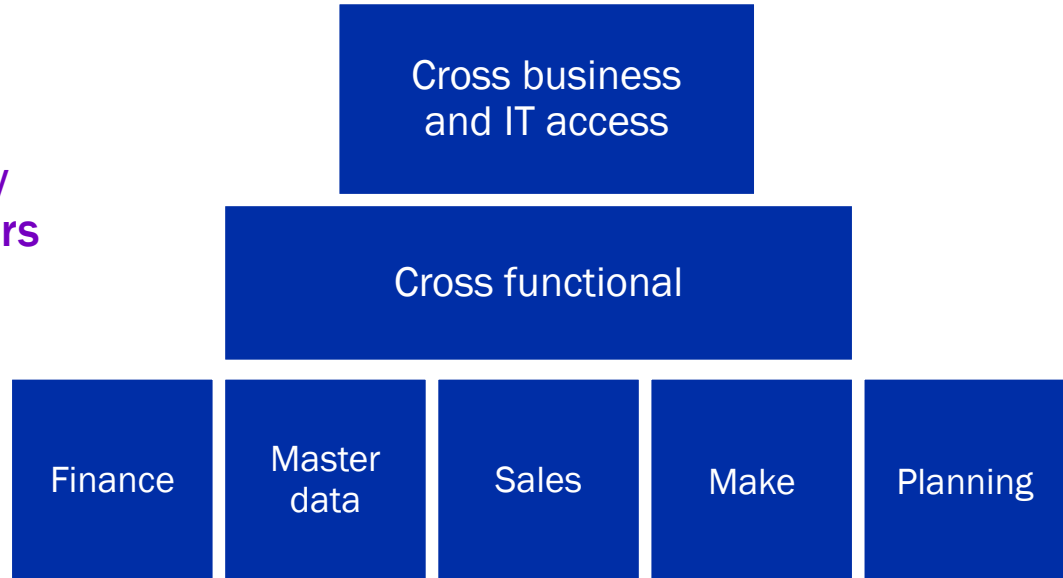
Benefits:

- Mitigates the most common open audit issue faced by virtually every company—elevated access assignment

Emergency Access Management (EAM)



The following structure may be used to design firefighters for EAM:



Emergency Access Management (EAM)

There are two ways of implementing firefighter:



Centralized emergency access management allows user to access firefighter IDs in plug-in systems from GRC Access control system. This avoids multiple logins in different systems.



Decentralized firefighting allows the user to leverage the emergency access management launchpad directly on the plug-in systems to perform firefighting.

Emergency Access Management (EAM)

The following are the approaches for emergency access assignment (Firefighter assignment) to users



On Demand firefighter access assignment:

Firefighter access will be assigned to users when required via Emergency access request process. The valid from and valid to dates are determined by the requestor/approver based on the activity performed.



Pre-Approved Firefighter assignments:

Firefighter access is assigned to users to check out when required. The access is generally set to expire end of the year. All existing firefighters are reviewed at the end of the year and extended as required.

Firefighter workflows

The following workflows may be configured for emergency access management:



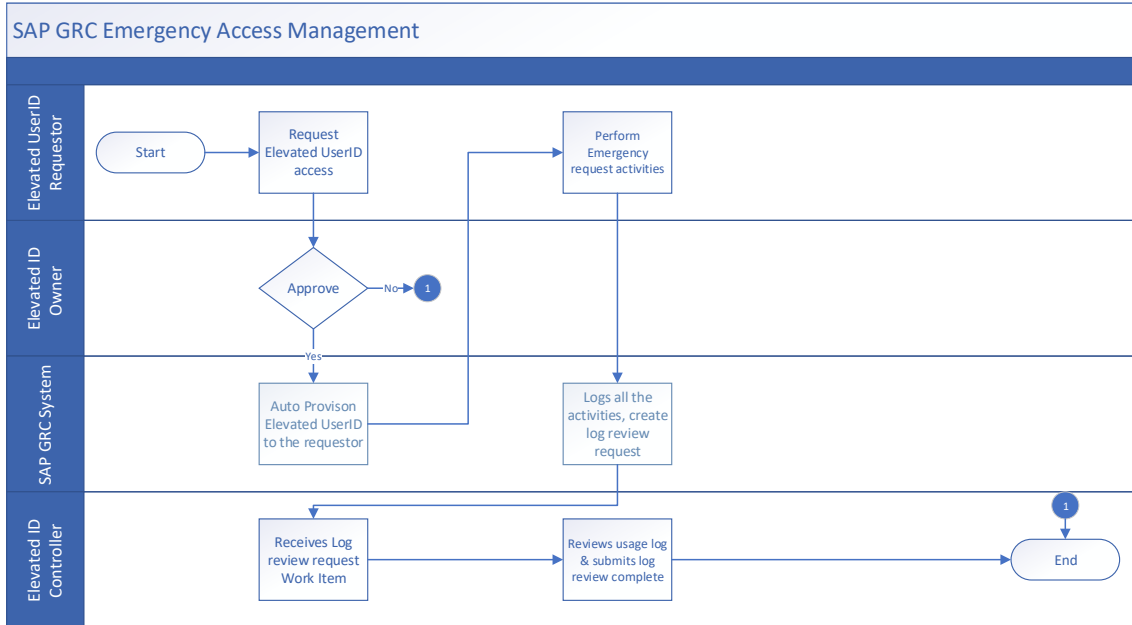
Emergency access provisioning



Emergency access monitoring
and usage log review

EAM: Sample workflow

The workflow below shows how EAM could work in your environment:



Business Role Management (BRM)

BRM is used for role creation, maintenance and built-in workflow routing/approval functionality.



Features:

- Central management of roles from multiple systems with a unified role repository
- Supports business role creation methodology and actions involved (e.g., define role, analyze access risk, request approval, provisioning)

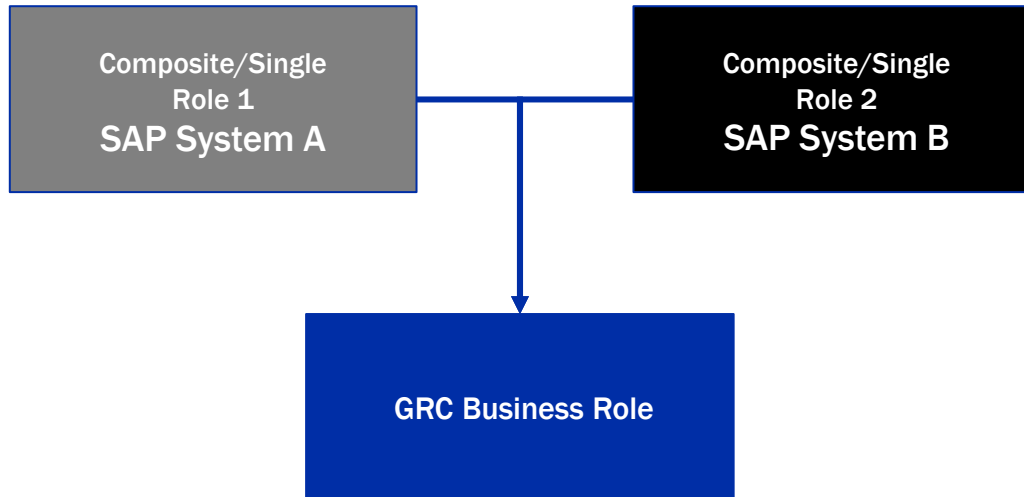


Benefits:

- BRM empowers role owners to be involved in the role-building process.

Business role functionality

GRC business role can encompass technical roles across multiple SAP systems.



BRM: Workflows

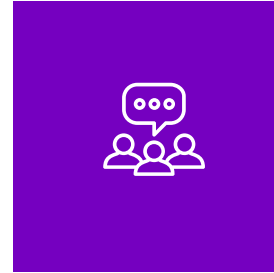
The following workflows may be configured for BRM:



**Create
roles**



**Change
roles**



**SOD analysis
at role level**

Access Request Management (ARM)

ARM provides a workflow engine to automate the user provisioning process.



Features:

- Automate User provisioning, deprovisioning and maintenance activities
- Mitigation of critical risk prior to user request approval

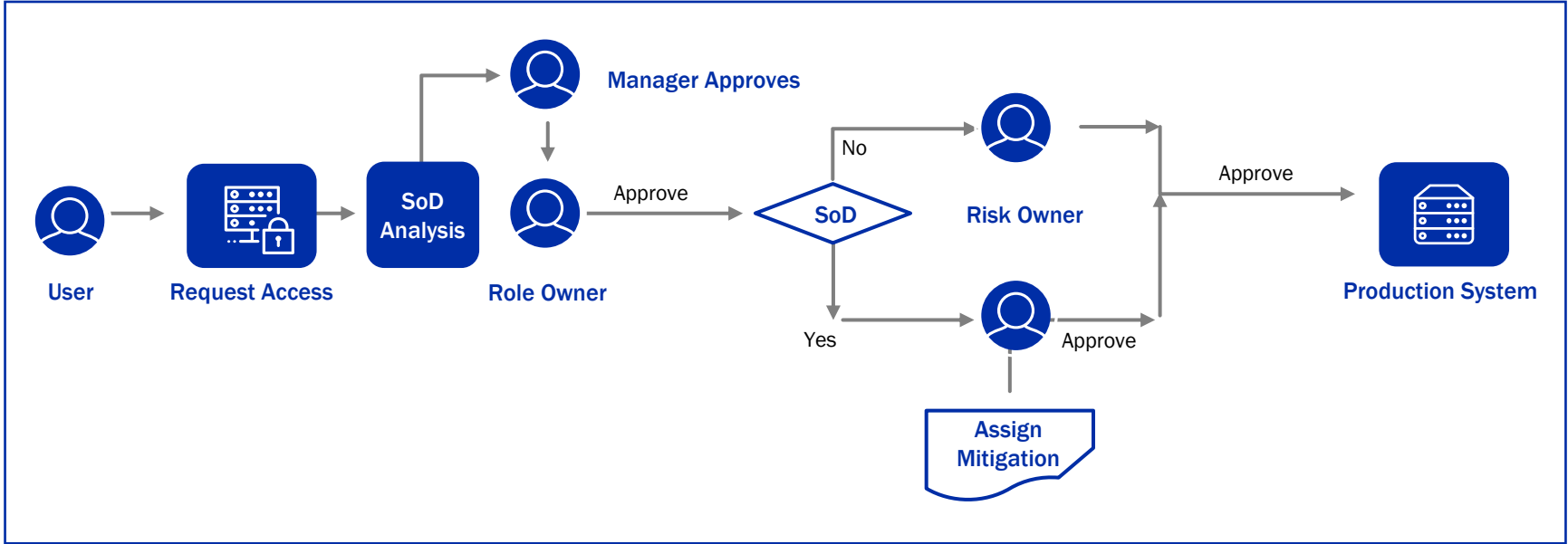


Benefits:

- Reduces manual effort involved in user provisioning
- ARM helps SAP system stay clean and in control
- Fiori enabled user interface for easy navigation

Sample ARM Workflow

Below is an example of the access request management process flow:



ARM Access request form

Access Request - Internet Explorer

Access Request

Submit

Close

Requestor **POLINED**

Reason for Request

* Description:

User Access Request

Request Details

* Request Type:

Access Request (IT S

* Request For:

Superuser Access

* User:

Access Request (IT Support)

SailPoint Provisioning Workflow

Priority:

User Lock

Business Process:

User Unlock

Functional Area:

User Delete

Due Date:

UMR Update

User Access

Risk Violation

Attachments

User Details

Parameters

User Groups

User System Details

Custom Data

Add

Remove

Existing Assignments

Import Roles

Simulation

Assignment	System	Type	Valid From	Valid To	Assignment...	Description	Comments	Provisionin...	Provisionin...	Provisionin...

59

SAPinsider

Access request management workflows

The following workflows may be configured for user provisioning / deprovisioning:



Create
user



Change
user



Unlock
user



Terminate
user



Password
change



Mitigation control
assignment to user



Preventive
SOD check

User Access Review (UAR)

UAR feature automates the periodic user access review performed by business managers and/or role owners.



Features:

- Automated process for periodic access review
- Workflow of requests for review and approval
- Status and history reports to assist in monitoring the review process



Benefits:

- A streamlined internal control process with collaboration among business managers, internal control, and information technology teams
- Improved efficiency and visibility of the internal control process
- Audit trail and reports for supporting internal and external audits

Types of User Access Reviews

Types of user access reviews performed within UAR:



Segregation of duties review

- Analyzes conflicting functions from the ARA ruleset. The purpose of the review is to remove or mitigate SoD conflicts.



Sensitive access review

- Analyzes users with access to critical SAP functions. The purpose of the review is to validate that only necessary personnel have access.

Types of User Access Reviews

Types of user access reviews performed within UAR:



Full user access review

- Analyzes the appropriateness of users and roles. The purpose of this review is to validate that a user's access is aligned with their job responsibilities, and that any unnecessary access is removed.

SAP Process Control (PC)

SAP PC automates control and compliance monitoring.
It is comprised of the following components:



Risk and
compliance
repository



Continuous
control
monitoring



Issue and
remediation
management



Compliance
evaluation



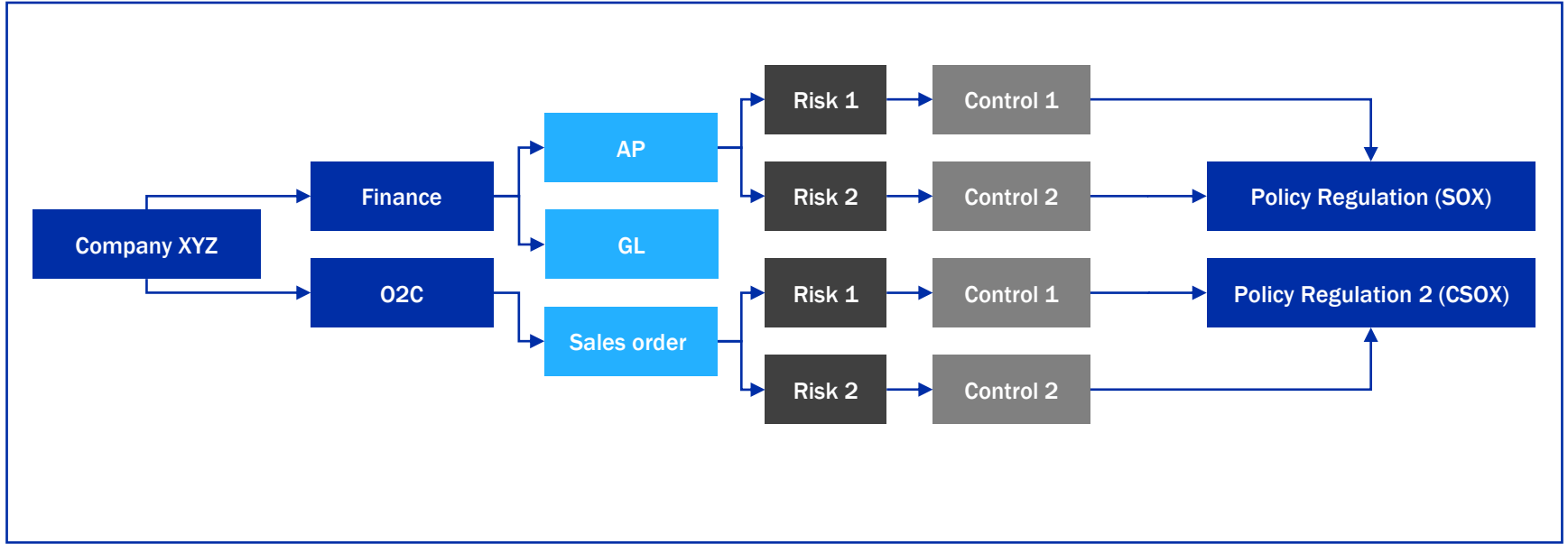
Policy and
procedure
maintenance



Reporting

Risk and compliance repository

The risk and control framework provides a central place to store an organizations controls.



Continuous Control Monitoring (CCM)

Use business rules to automate control testing related to system configuration, master data, security and transactional data.



Features:

- Monitor master data, configuration settings and transactions in business applications via scheduled processes or in real-time
- Use MSMP workflow to support the alerts, reviews, approvals, and other process automation needs
- Continuously monitor SODs through AC-PC integration

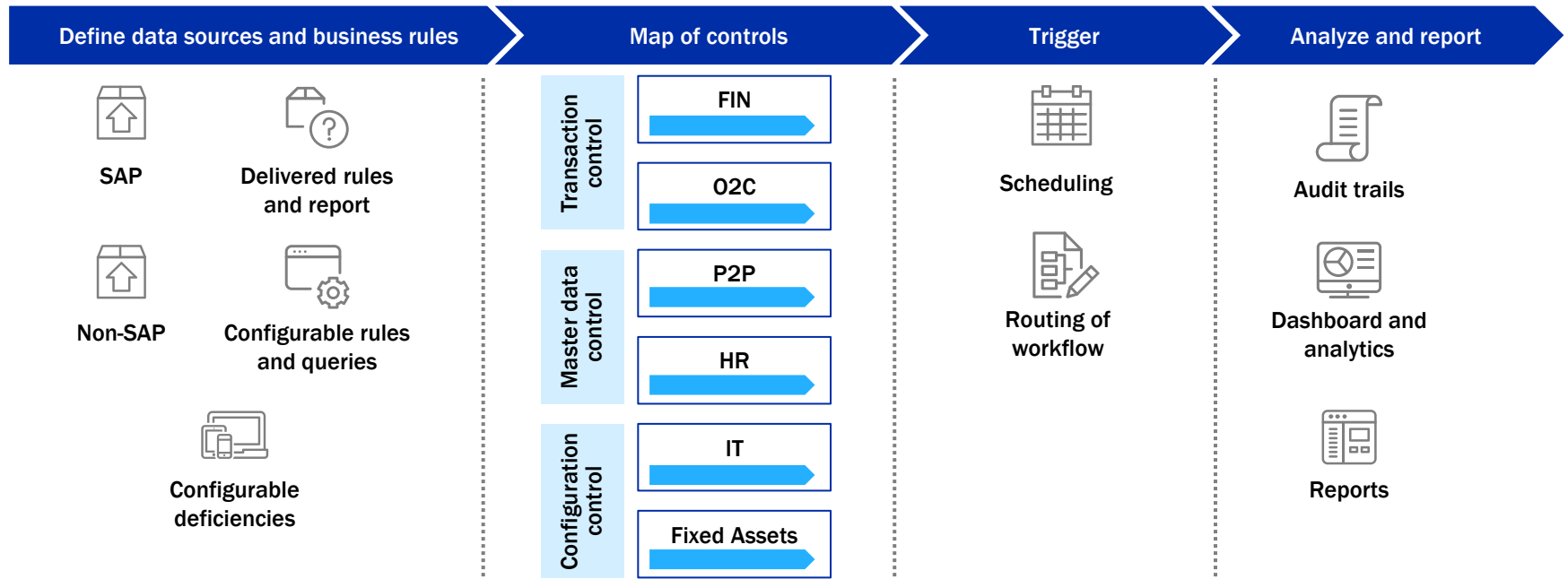


Benefits:

- Automated key compliance and control activities to prioritize resources and reduce costs
- Continuous insight into the status of compliance and controls for faster, more effective action

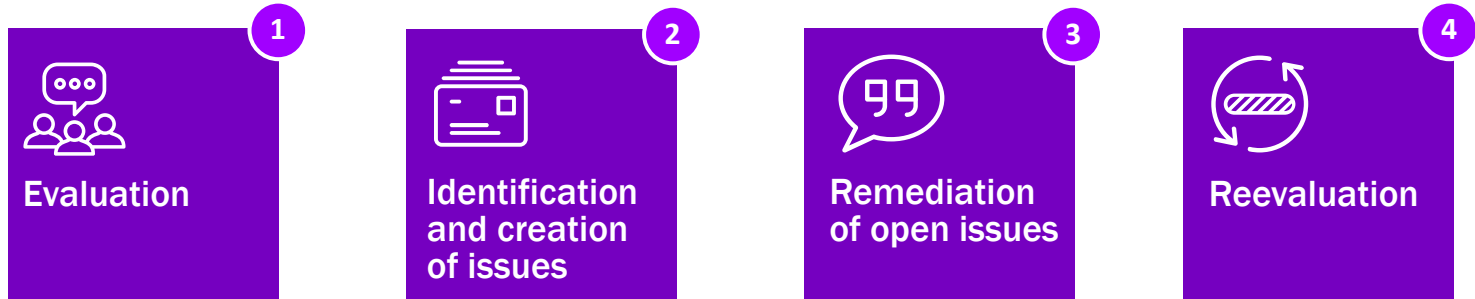
SAP PC: Designing CCM

The process for continuous control monitoring:

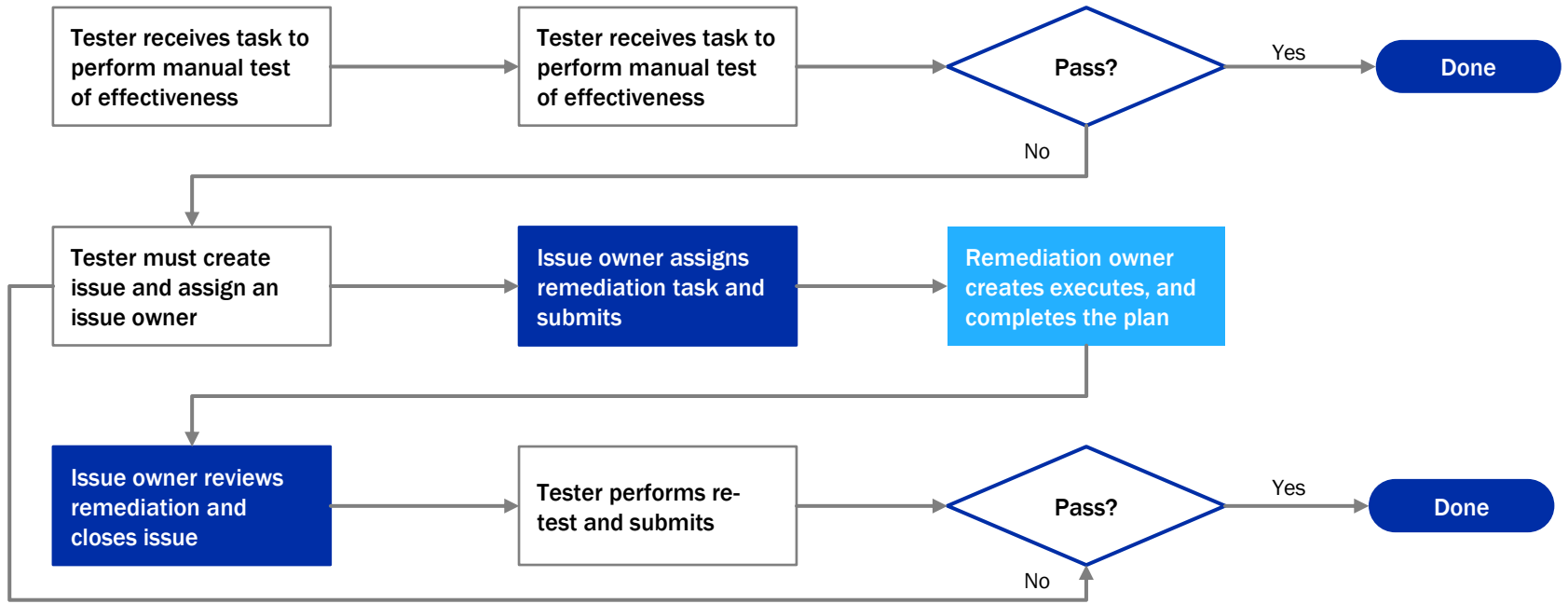


Issue and remediation management

Automate and predefine workflows to track issue remediation plans and associated activities

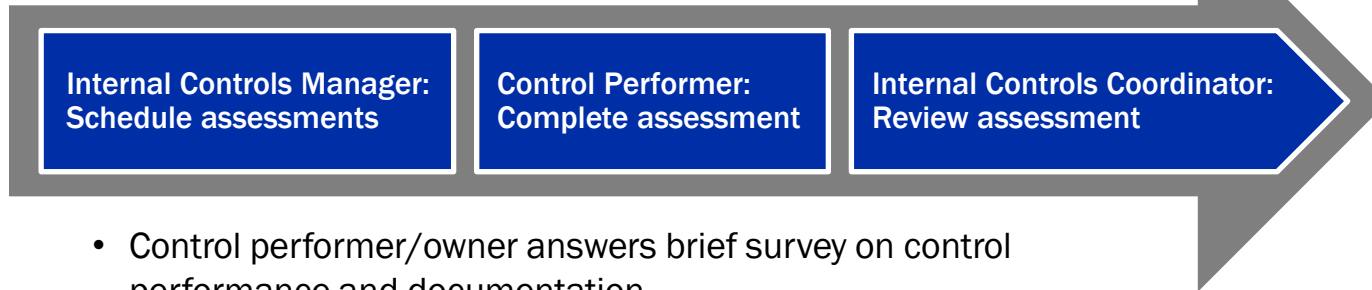


Issue and remediation management



Compliance evaluation - Assessments

PC Assessments allow the design and effectiveness of controls to be tracked across the organization



- Control performer/owner answers brief survey on control performance and documentation
- Leverage process control native “self-assessment” workflow
- Custom-configure a PC report for easy results compilation



A control owner completes a self assessment for the effectiveness of controls.

Other Process Control (PC) Capabilities



Sign-off / Certification

SAP PC offers sign-off functionality to formalize accountability for the status of internal controls across the organizational hierarchy



Policy and Procedure Maintenance

GRC PC manages the life-cycle of policies from creation to publishing to distribution



Reporting

Drill-down capabilities around master data, testing results, issues/ remediation, assessment surveys, continuous controls monitoring, user access are delivered by SAP

SAP Identity Access Governance (IAG)

SAP IAG is a cloud-based application and is often referred to as access control for cloud systems.



Features:

- End-to-end access governance capabilities
- Risk-driven approach for determining access
- Auditable workflow, integrated risk analysis, and compliance related approvals
- Ability to manage access for on-premise and cloud applications
- Designed for a cloud first strategy
- Fiori based user experience

SAP Identity and access governance components



Access
analysis



Role
design



Access
request



Access
certification



Privilege access
management

SAP Identity and access governance vs GRC 12

Functionalities supported by IAG and GRC:

Functionality	GRC 12 (on-prem)	IAG (on-prem & cloud)
Access request provisioning for SAP on premise		
Access request provisioning for SAP cloud		
Emergency access management		ABAP systems only
Access risk analysis		
Access certification (UAR)		
Role design		
Process control		
Risk management		

Comparison of GRC and IAG components

SAP access control module		SAP IAG module
Access risk analysis	➡	Access analysis
Business role management	➡	Role design
Access request management	➡	Access request
Emergency access management	➡	Privileged access management
User access review and SOD risk review	➡	Access certification

****GRC is more customizable compared to IAG ****

IAG Standalone vs. IAG Bridge



Cloud driven/stand alone approach:

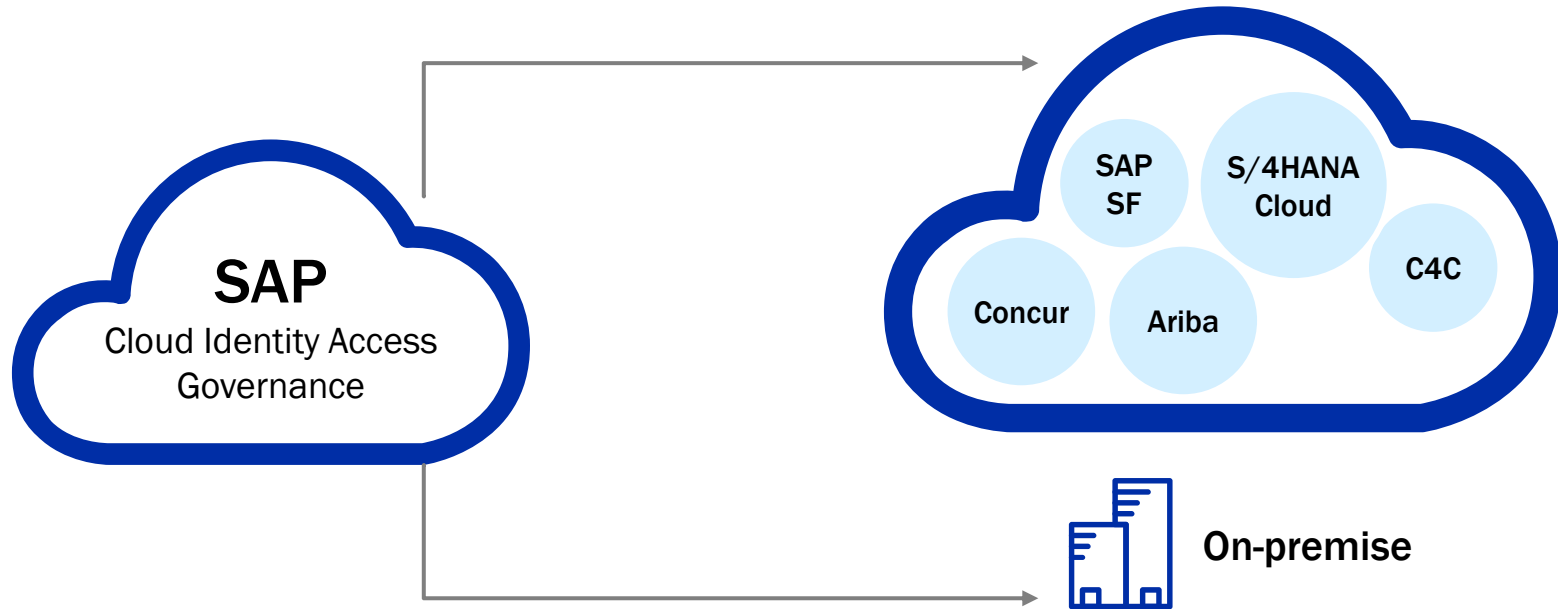
- IAG is used to govern on premise and cloud applications without SAP access control



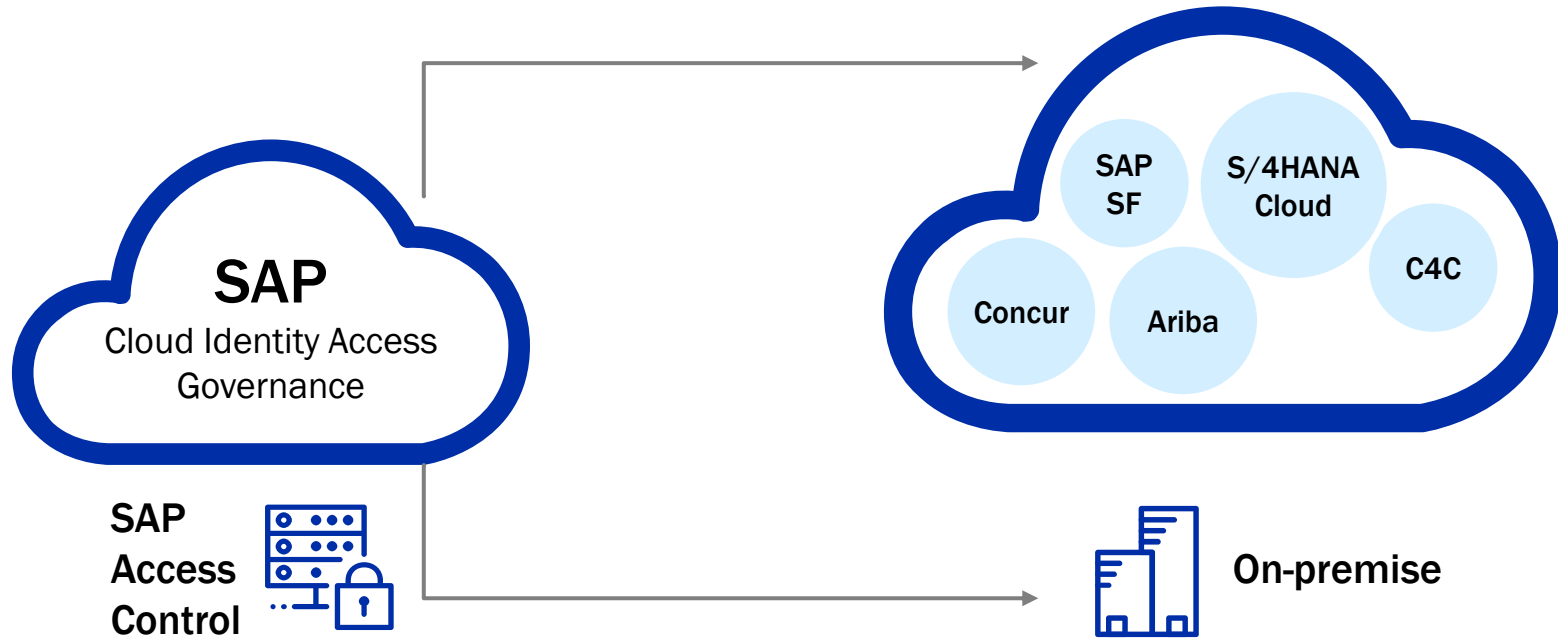
Hybrid approach:

- SAP IAG allows you to extend your SAP GRC access control to manage hybrid SAP landscapes with the IAG bridge functionality.
- Bridge functionality helps leverage SAP access control existing functionality to customize workflows

IAG Standalone



IAG Bridge



Identity management – SAP GRC Integration

SAP GRC can be integrated with corporate identity solutions (SAP IDM, Sailpoint)



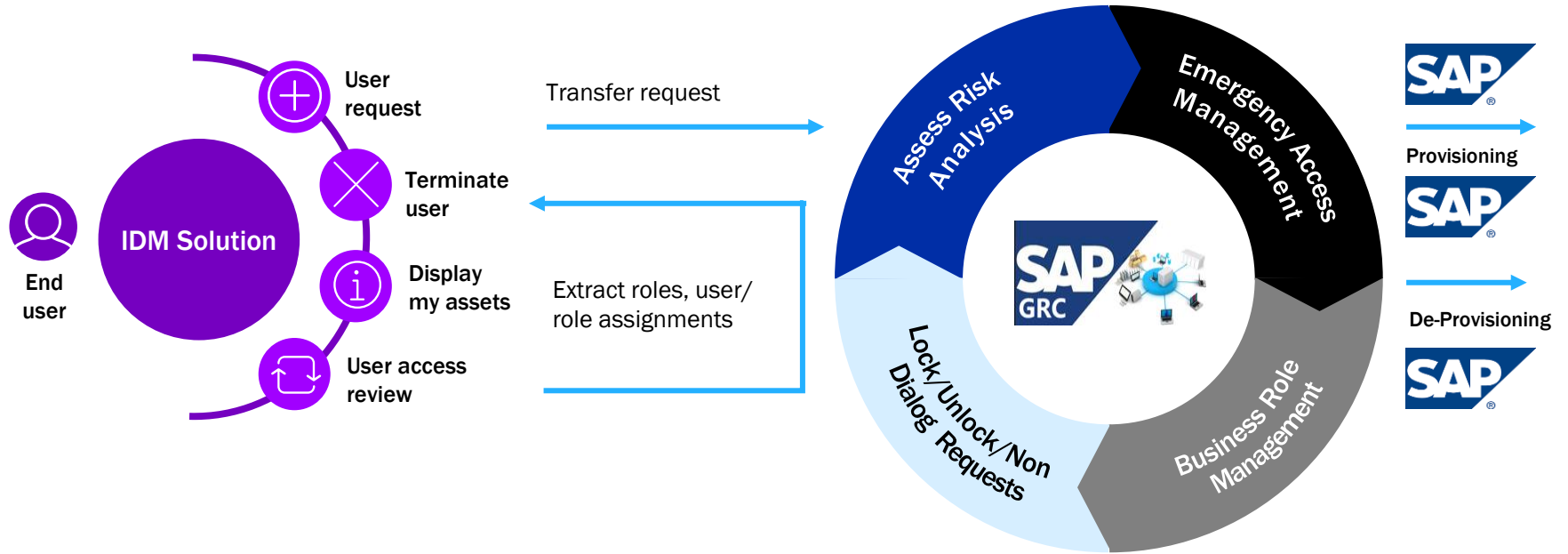
Benefits:

- Single user interface for employees to request or review application and/or system access, creating a one-stop-shop for all enterprise user access needs
- 360-degree view of user access and activity across the enterprise, especially to systems that hold critical or sensitive information
- Detective and preventive policy enforcement for separation of duties (SoD) across application boundaries

IDM and SAP Integration

	 Logical separation of company's roles & user identities	 Centralized system for access requests	 SoD validation on SAP system	 Centralized access certification	 Audit trails
IdM Only	✓	✓	✗	✓	✓
SAP GRC	✗	✗	✓	✗	✓
IdM + SAP GRC	✓	✓	✓	✓	✓

IDM and SAP Integration



What we'll cover

- **SAP Security and GRC – Why important?**
- **Introduction to SAP Security**
 - How security works in SAP
 - Differences between SAP ECC and S/4 HANA
 - Key design methodologies
 - Security key performance indicators / governance
- **Introduction to SAP GRC**
 - SAP Access Control (AC)
 - SAP Identity and Access Governance (IAG)
 - SAP Process Control (PC)
- **Introduction to SAP Cyber Security**
- **Wrap up**



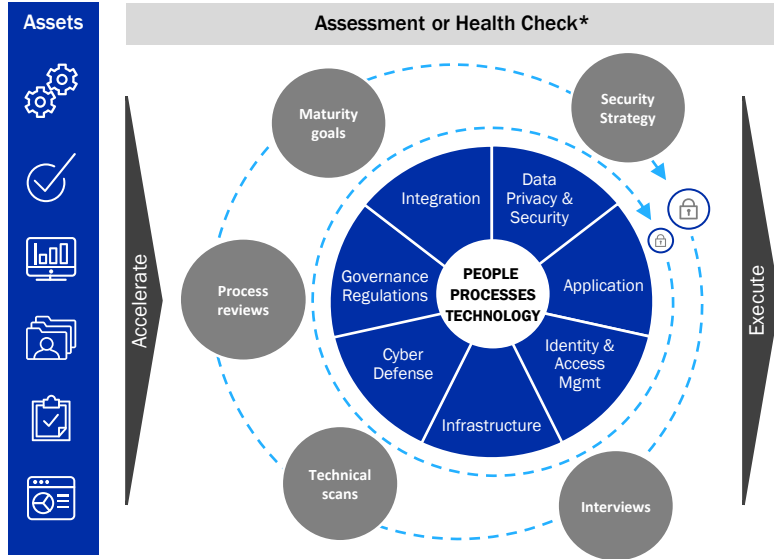
Comprehensive enterprise approach for your SAP Program

► Define & assess service baseline

► Review security consideration

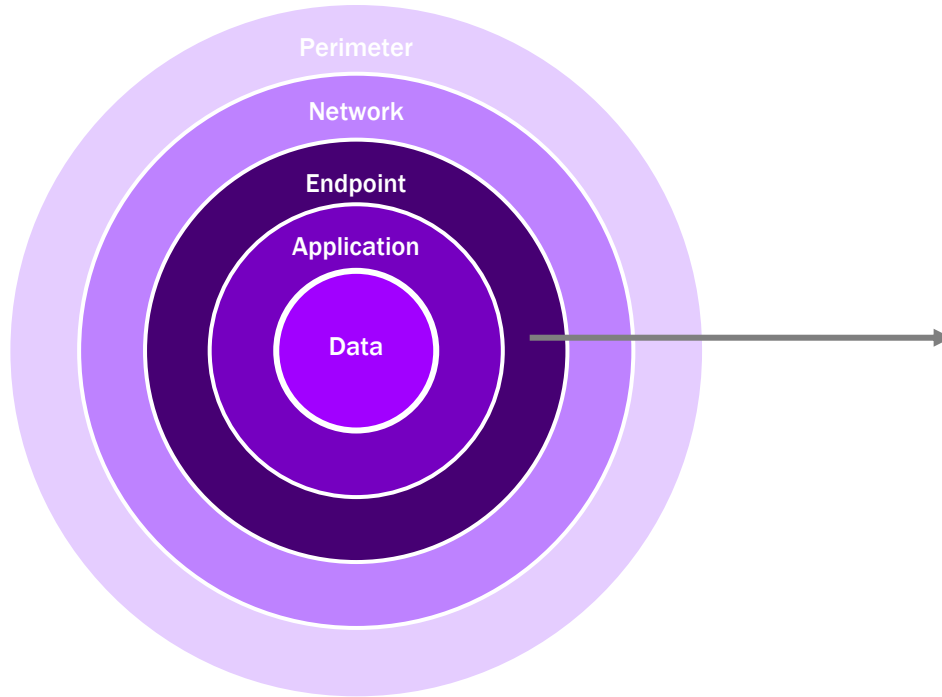
► Map service

► Run services



Security considerations					Integrated Delivery Model	Managed Security Services
Integration	Application		Data Privacy & Protection			
Executive reporting & analytics	User & Authorizations Mgt.		Data Discovery & Classification			
	Security Logging & Monitoring		Data Access Controls			
Central Network Mgt.	Update & patch management		Data Encryption			
	Governance Risk & Compliance solutions		Data Masking			
Certificate Authority	Segregation of Duty (SoD) & Critical access		Data Archiving & Deletion			
	System Hardening		Certificates and Key Mgt.			
Cloud Security Service Catalogue	Security Testing		Data Access Audit			
	Business Control Validation & Automation		Data Loss Prevention			
Provisioning & Orchestration	DevSecOps Application Code Scanning SAP Transport Management Container Security Secure Code Development		Identity & Access Management			
			Identity Lifecycle Management			
SOD Management Integration			User Access review			
			Emergency Access Mgmt.			
Privilege Access Mgt Integration			Role Management			
			Identity Intelligence (AI)			
Identity Mgt. Integration			Authentication (SSO & MFA)			
			Privileged Access Management			
SAP Event & SIEM Integration	Cyber Defense & Resilience		Incident Response / XDR & Forensics			
	Threat Mgt. & testing		Threat Monitoring & Hunting			
SAP GRC/IAG Integration	Cyber Threat Intelligence		Vertical - Cyber Security Architecture			
	Vulnerability Mgt.					
	Hybrid infrastructure		Server/Endpoint (e.g. antivirus)			
	Resilience, BC,DR		Malware & Ransomware Protection			
	KMS / Encryption		Posture Management			
	Asset Protection					
	Strategy, Governance & Awareness & Design		Security Prg. & Framework			
	Awareness Training		Strategy & Roadmap			
	Compliance Advisory		Project Risk Mgt.			
			Design Authority			

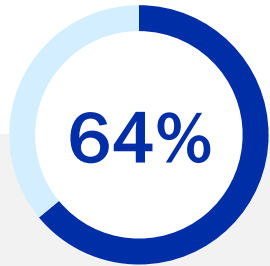
SAP Cyber security – Why important?



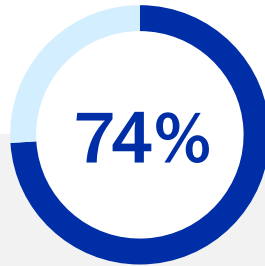
In many organizations, the application layer is neglected by typical information security processes

SAP Cyber Security – Why important?

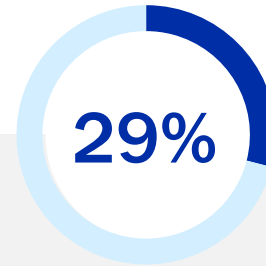
The threat from cyber attack is one of the top risk factors:



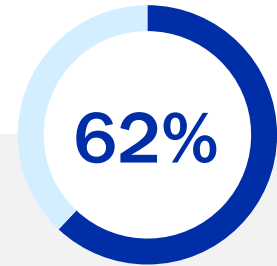
Of companies have had their ERP system breached in the last **2 years**



Of companies' ERP systems are accessible **via the internet**



Of companies report downtime would cost **\$100k+ per HOUR**



Of companies believe their ERP systems have **critical vulnerabilities**

10K Blaze example



10K Blaze is a known, high-risk vulnerability that can result in potential financial risk if not remediated.

US-CERT Alert (AA19-122A)

New exploits for unsecure
SAP systems



10K Blaze example



10K Blaze is a known, high-risk vulnerability that can result in potential financial risk if not remediated.

THREAT REPORT

10KBLAZE

Protection From a Cyber
Exploit with the Power to
Burn Financial Statements

SAP Cyber security – Why important?

SAP normally houses your most critical information:



**Customer
Master Data**



**Vendor Master
Data**



**Financial
Information**



**Personnel
Records**



Yet many times, SAP is not subject to standard information security programs that many CISOs implement for their organizations (e.g. “SAP in a Silo”)

Key SAP Cyber security considerations

SAP Cyber Security typically refers to:



Patch
management



ABAP code
scanning



System
hardening



Threat
modeling



Network
security

Breach considerations

Most breaches occur because of:



Lack of
patching



Inappropriate
configurations



Most breaches are not complex. They typically occur because preventable actions were not taken by the system owner.

Know your information assets

In most SAP systems, critical information assets exist, such as the following:



Bill of
material



Financial
data



Product
specifications



Margins



Personnel
data



Do you have an information security plan to protect these? Do you have the correct preventative and monitoring tools to avoid losses?

What we'll cover

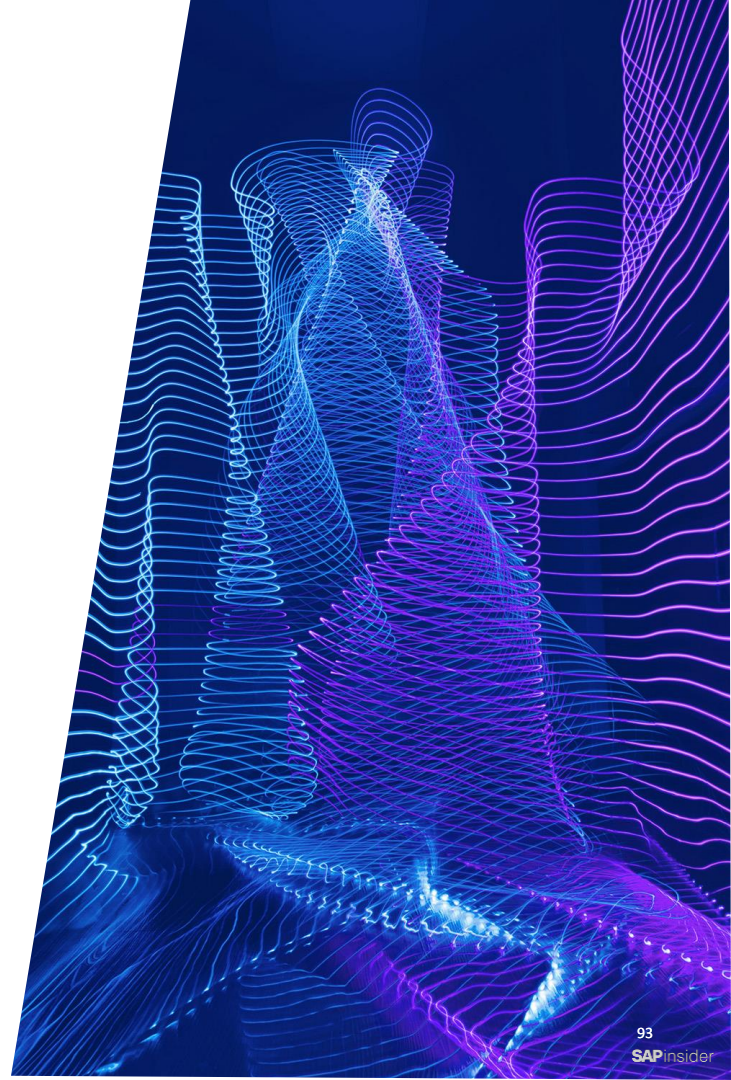
- **SAP Security and GRC – Why important?**
- **Introduction to SAP Security**
 - How security works in SAP
 - Differences between SAP ECC and S/4 HANA
 - Key design methodologies
 - Security key performance indicators / governance
- **Introduction to SAP GRC**
 - SAP Access Control (AC)
 - SAP Identity and Access Governance (IAG)
 - SAP Process Control (PC)
- **Introduction to SAP Cyber Security**
- **Wrap up**



Key points to take home



- The landscape of SAP Security is changing, which introduces new complexities requiring consideration.
- SAP AC's ARM and BRM functionalities can be used to bundle Fiori, S/4 and HANA entitlements into business roles for end users.
- SAP PC's CCM functionality is a powerful tool and should be utilized to improve control monitoring efficiency.
- SAP is a target for cyber criminals because of its information assets. internal threats must be considered.
- Breaches related to SAP are typically coming from simple fixes that can be handled via strong processes.



Where to find more information

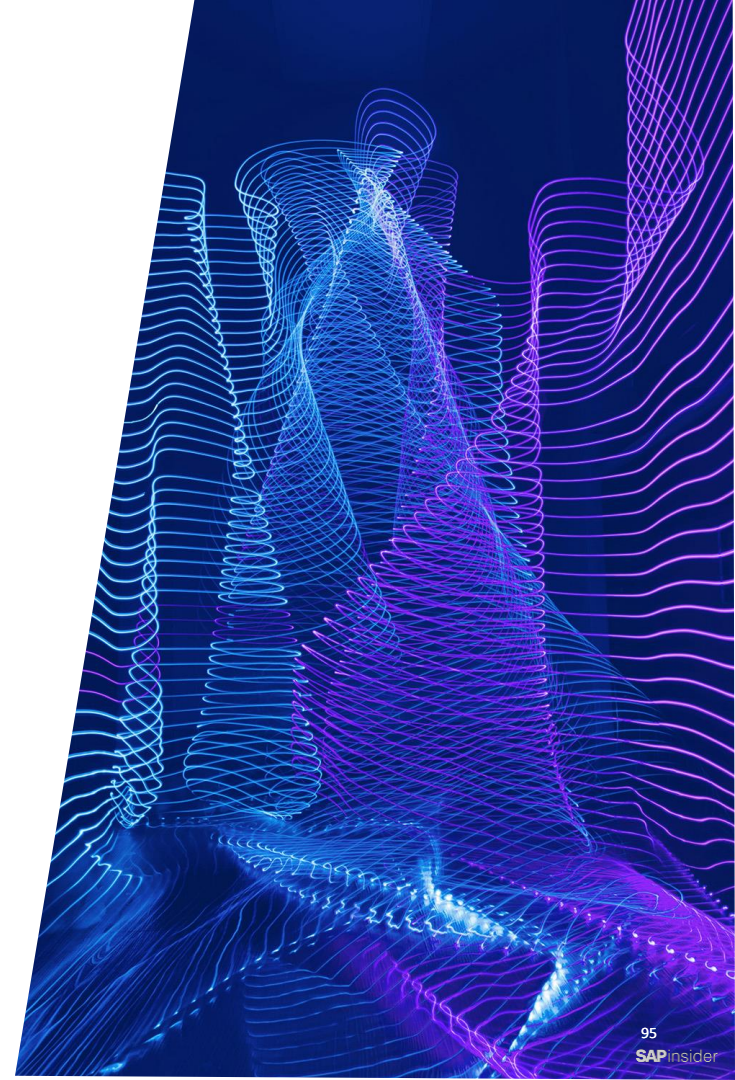
- https://help.sap.com/doc/eec734dbb0fd1014a61590fcb5411390/2.0.05/en-US/SAP_HANA_Security_Guide_en.pdf
 - SAP S/4 HANA Security Guide - 2022
- https://www.accenture.com/us-en/insights/security/cyber-threat-intelligence-report-2021-vol-2?c=acn_glb_brandexpressiongoogle_12906185&n=psgs_0322&gclid=Cj0KCQjwnNyUBhCZARIsAl9AYlERT5yujbID9mzq-k65II5oEd7RJRGg71oeGTs_HJw3zmLksR7zriYaAvfZEALw_wcB&gclsrc=aw.ds
 - 2022 Accenture Cyber Security Threat Report
- <https://onapsis.com/resources/10kblaze>
 - 10k Blaze Threat Report
- <https://www.gartner.com/doc/reprints?id=1-26IYZ4BR&ct=210615&st=sb>
 - Gartner Magic Quadrant for SAP S/4 HANA Application Services

Thank you! Any questions?

Ray Mastre

Ray.Mastre@Accenture.com

 <https://www.linkedin.com/in/raymastre/>





SAPinsider.org

PO Box 982Hampstead, NH 03841
Copyright © 2023 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 worldwide, with more than 600,000 members across 205 countries.
