SAP S/4HANA SECURITY & GRC 12.0 ROUNDTABLE

Hosted by Protiviti & SAP

Tuesday, November 13, 2018

Protiviti Perspective provided by Michael K., New York

Internal Audit, Risk, Business & Technology Consulting

AGENDA

8:00 AM 01 Check In & Breakfast

9:00 AM 02 Introduction

03 Intelligent Enterprise and S/4HANA – **SAP**

04 Key Considerations for S/4 Security – **Protiviti**

05 Giveaway Drawing

10:00 AM 08 What's New with GRC 12.0 – **SAP**

09 IAG Overview and Demo – **SAP**

10 The Road Ahead – **Protiviti**

11 Client Spotlight – **Tapestry, Inc.**

12 Wrap up / Q&A

KEY SPEAKERS

Peter Creal

SAP

Senior Director,
GRC

peter.creal@sap.com

Phil Jacobs

SAP

Account Executive

p.jacobs@sap.com

Host

Sarma Adithe

SAP

Chief Product Owner,
Access Control

sarma.adithe@sap.com

Kyle Wechsler

Protiviti

Director,
ERP Solutions

kyle.wechsler@protiviti.com

Madhu Mathew

Protiviti

Associate Director,
ERP Solutions

madhu.mathew@protiviti.com

Toni Lastella

Protiviti

Managing Director,
ERP Solutions

toni.lastella@protiviti.com

Host

Suketu Patel

Tapestry, Inc.

Director, IT Risk and
Compliance

spatel2@tapestry.com

protiviti®

SAP® tapestry

Intelligent Enterprise and S/4HANA

Peter Creal, SAP
November, 2018

PUBLIC

THE BEST RUN SAP

The Intelligent Enterprise Accelerates Value Creation

Capabilities

Visibility

the ability to collect and connect data that was previously siloed and recognize unseen patterns

Focus

the ability to simulate the impact of potential options and direct scarce resources to the areas of maximum impact

Agility

the ability to respond faster to changes in the marketplace or the business and pivot business processes towards the right customer outcomes

Outcomes

Do more with less and empower employees

through process automation and freeing up people to do more meaningful work

Deliver best-in-class customer experience

by anticipating and proactively responding to end-customer needs

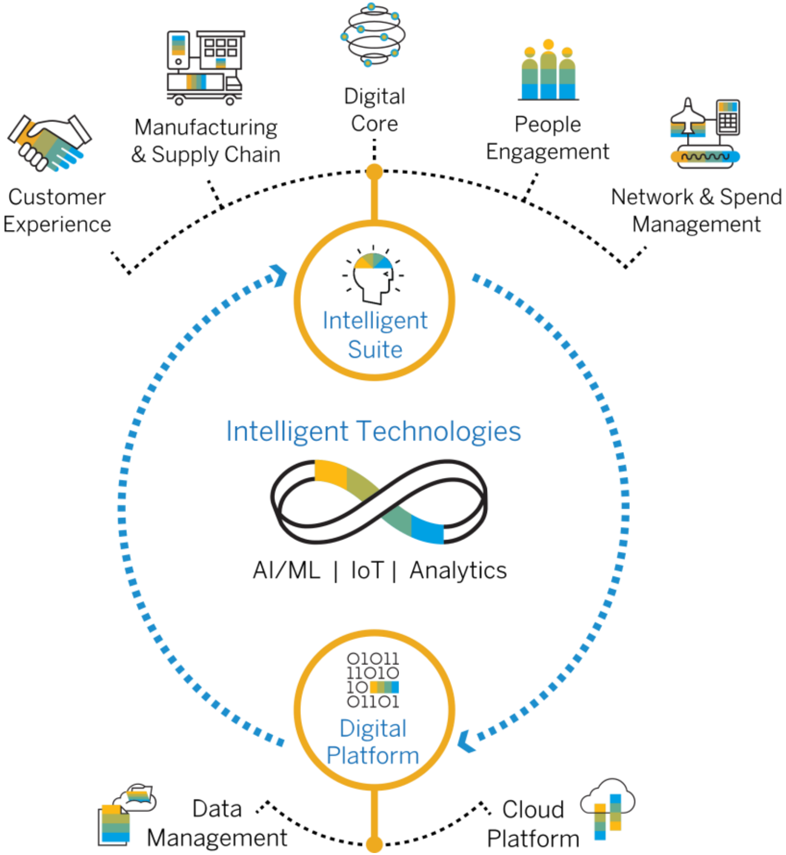
Invent new business models and revenue streams

by monetizing data-driven capabilities and applying core competencies in new ways

SAP Strategy – Deliver The Intelligent Enterprise

THE INTELLIGENT ENTERPRISE

features **3 KEY COMPONENTS:**

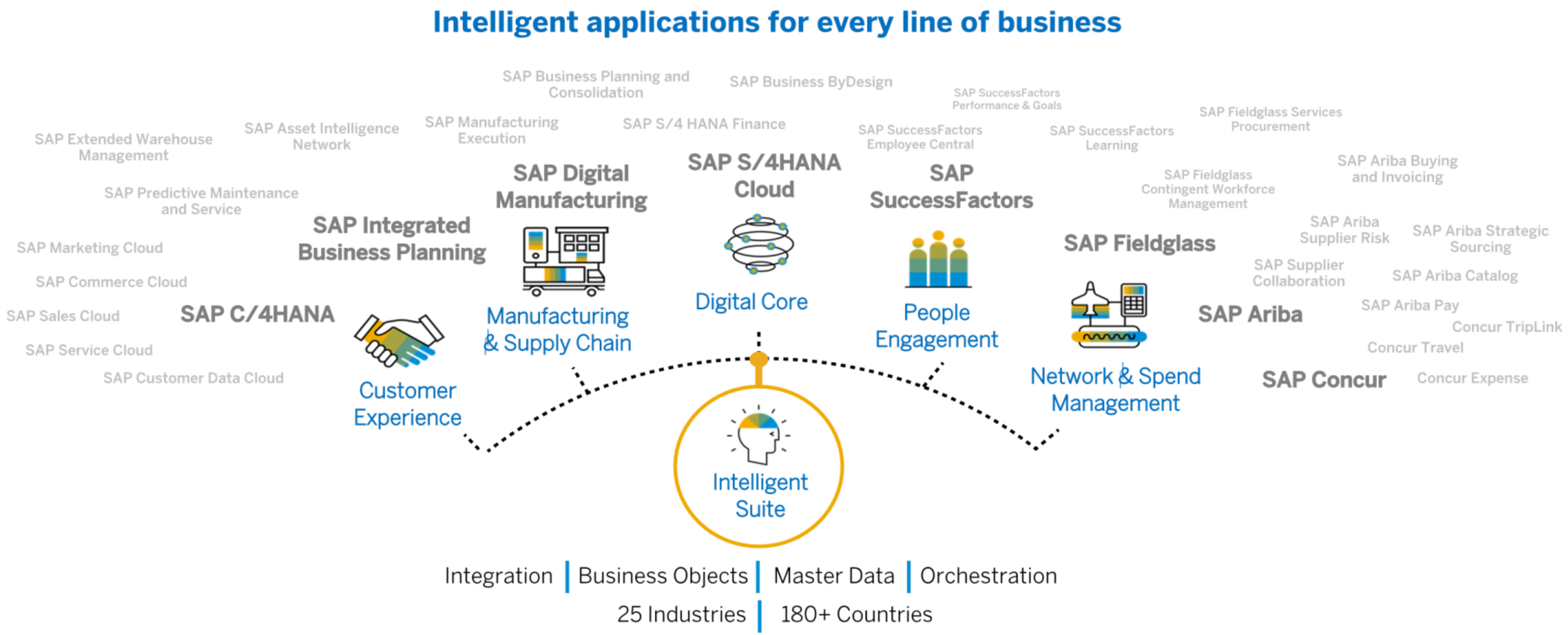


1 Intelligent Suite

2 Digital Platform

3 Intelligent Technologies

Intelligent Suite: Deliver Intelligence Across Value Chains


Intelligent applications for every line of business
SAP Business Planning and Consolidation
SAP Business ByDesign
SAP SuccessFactors Performance & Goals
SAP Fieldglass Services Procurement
SAP Extended Warehouse Management
SAP Asset Intelligence Network
SAP Manufacturing Execution
SAP S/4 HANA Finance
SAP SuccessFactors Employee Central
SAP SuccessFactors Learning
SAP Ariba Buying and Invoicing
SAP Predictive Maintenance and Service
SAP Digital Manufacturing
SAP S/4HANA Cloud
SAP SuccessFactors
SAP Fieldglass Contingent Workforce Management
SAP Integrated Business Planning
SAP Ariba Supplier Risk
SAP Ariba Strategic Sourcing
SAP Marketing Cloud
SAP Fieldglass
SAP Supplier Collaboration
SAP Ariba Catalog
SAP Commerce Cloud
SAP Sales Cloud
SAP C/4HANA
Manufacturing & Supply Chain
Digital Core
People Engagement
SAP Ariba
SAP Ariba Pay
Concur TripLink
SAP Service Cloud
Concur Travel
SAP Customer Data Cloud
Customer Experience
Network & Spend Management
SAP Concur
Concur Expense
Intelligent Suite
Integration | Business Objects | Master Data | Orchestration
25 Industries | 180+ Countries

Out-of-the-box integration leveraging SAP Cloud Platform, the SAP Analytics Cloud solution, and a common data foundation with SAP HANA and SAP Data Hub

Best-in-class UX with **consistent experience** across the entire portfolio

Modular, making it easy to consume and cost-effective to operate.

Easy to extend, allowing customers and partners to customize solutions quickly

Intelligence embedded in the applications making the workflows smarter

Digital Platform: Unlock Data-Driven Intelligence And Innovation

Unified data management to capture real-time value from different types of data

Meta Data and lifecycle management

SAP Data Services

Smart data Integration

SAP CP Big Data Services

SAP Data Hub

Integration services

Object Store (S3, Swift…)

SAP HANA Engines

SAP HANA

Smart data access

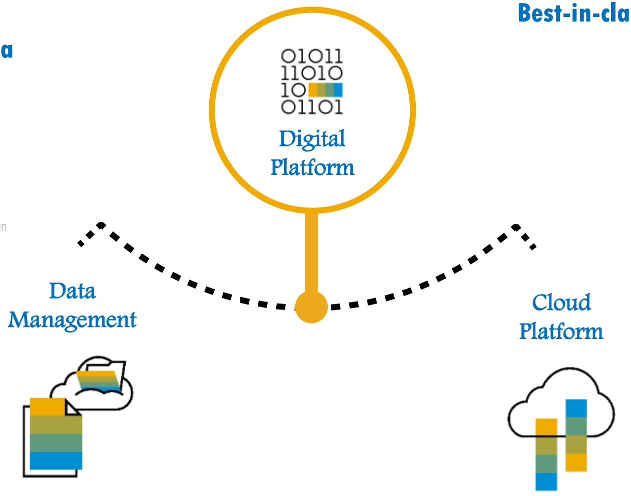
Orchestration and governance

Streaming analytics

Third party (Spark/Hadoop)

Data Lifecycle Management

SAP Vora distributed engines



Best-in-class digital platform for new app development, extensions, and integration

Marketplace

Collaboration Services

Portal

SAP Cloud Platform

Mobile Services

UX Services

SAP API Business Hub

Big Data Services

Leonardo IoT Services

API Management

Security Services

Analytics Services

Integration Services

Leonardo ML Services

Next-generation data management expands SAP HANA in-memory database to address **structured and unstructured data use cases and external data**

SAP HANA powers SAP applications as the foundation of **high-performance data warehousing** and analytics

SAP Data Hub provides **data orchestration and metadata management** across heterogeneous data sources

Platform for **extending the business processes** of the Intelligent Suite and enabling new innovations

Delivering deep data and process integrations through **APIs and microservices**

Marketplace for ecosystem to build new innovations leveraging APIs and business services

Intelligent Technologies: SAP Leonardo Everywhere

Core Applications
SAP Leonardo embedded

SAP Intelligent Cash Management

SAP Service Ticket Intelligence

SAP Brand Intelligence

SAP Customer Retention

SAP Resume Matching

SAP Global Track and Trace

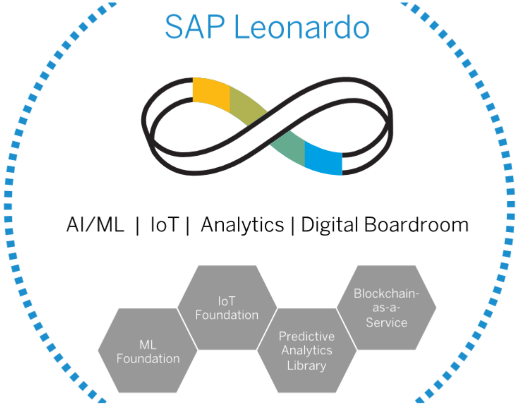
SAP Predictive Engineering Insights

SAP Vehicle Insights

SAP Manufacturing Execution

SAP Asset Intelligence Network

SAP Predictive Maintenance and Service



SAP Leonardo

AI/ML | IoT | Analytics | Digital Boardroom

IoT Foundation

Blockchain-as-a-Service

ML Foundation

Predictive Analytics Library

Industry Innovation Kits
Industry-led SAP Design Thinking Methodology

Solution Ideation & Vision 〉 Rapid Prototyping 〉 Integration Blueprint 〉 Business Case Development

Discrete Manufacturing Logistics and Spare Parts

Discrete Manufacturing Service and Assets

Chemicals Spare Parts

Chemicals Service and Assets

Utilities Service and Assets

Consumer Products Assets and Logistics

Travel and Transport Logistics

Retail Assets and Logistics

Applications that deliver **intelligence within core business process** (such as intelligent ERP, ERP, intelligent HR)

A **toolbox of intelligent technologies** (IoT, AI/ML, and analytics), microservices, and data management tools that will be available over SAP Cloud Platform to deliver intelligence out of the box as well as through co-innovation

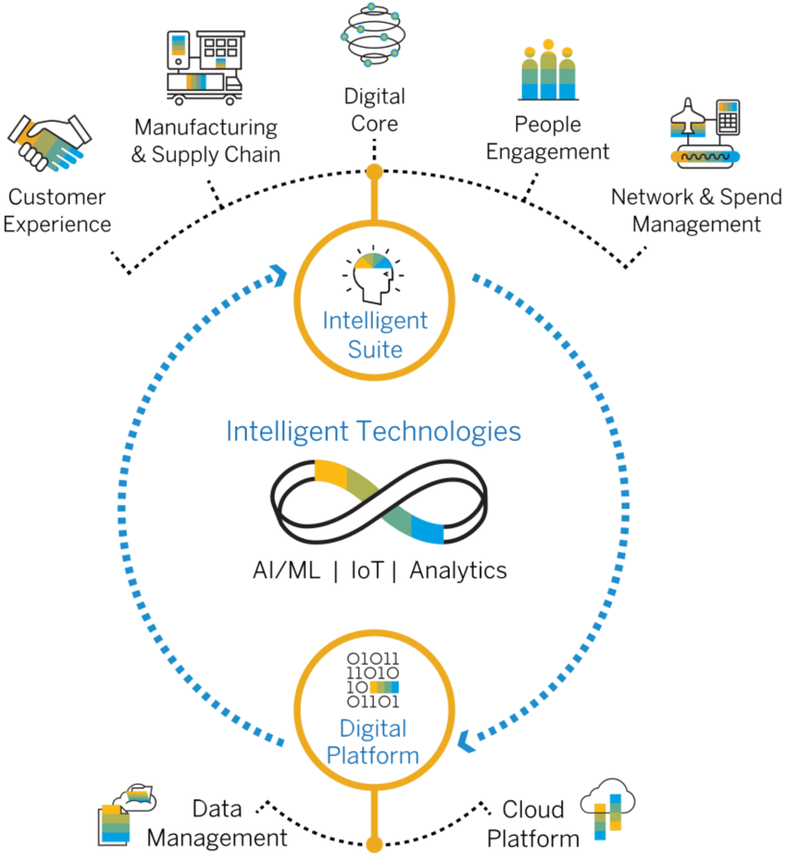
Universal analytics and SAP Digital Boardroom solution connecting the enterprise for the CXO

Innovation services combining design-thinking and industry accelerators to help ensure customers derive value from innovative new technologies quickly and with reduced risk

SAP Strategy – Deliver The Intelligent Enterprise

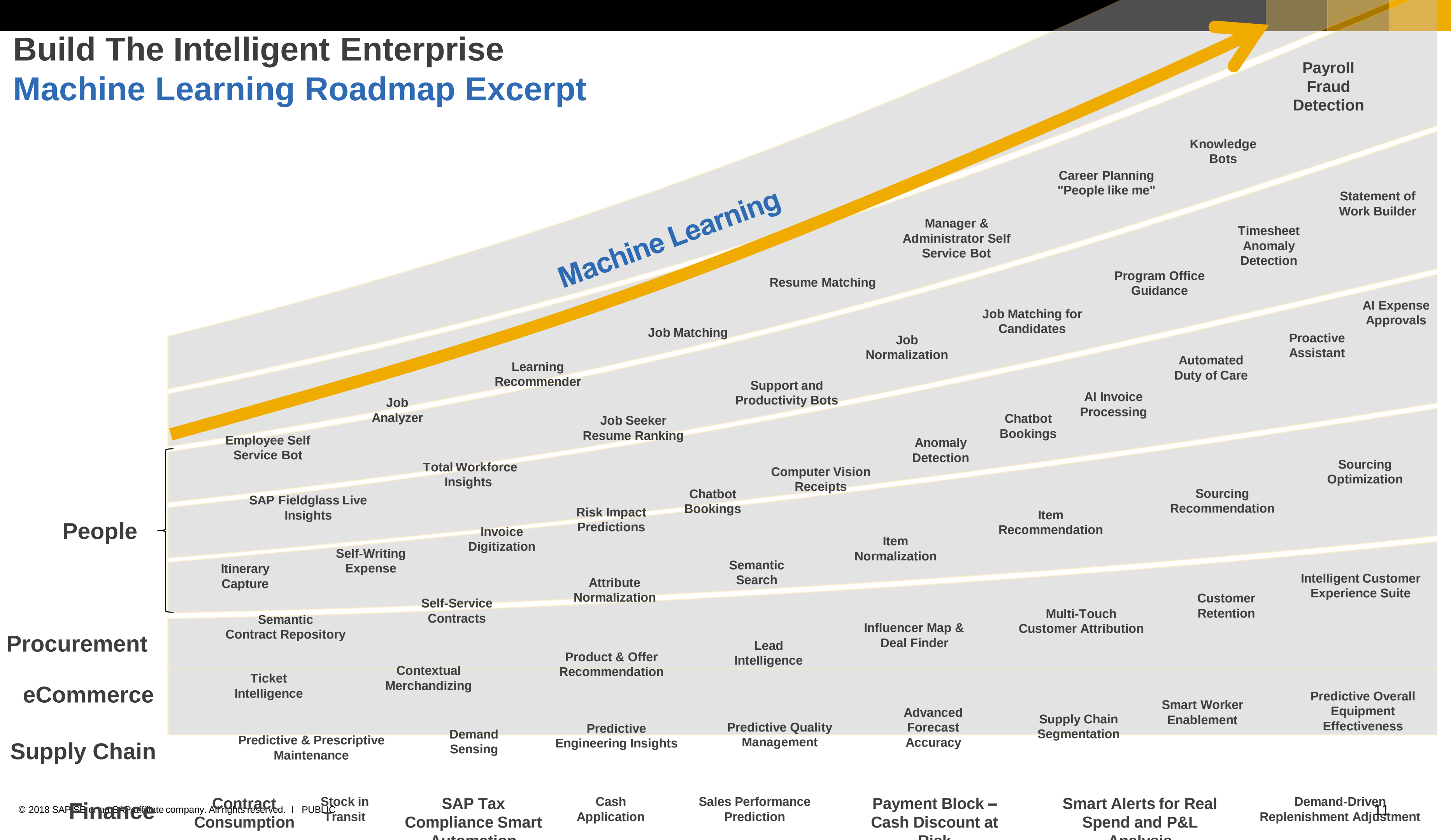
THE INTELLIGENT ENTERPRISE

features **3 KEY COMPONENTS:**



1. Intelligent Suite
2. Digital Platform
3. Intelligent Technologies

Build The Intelligent Enterprise
Machine Learning Roadmap Excerpt



Machine Learning

People

Employee Self Service Bot
Job Analyzer
Learning Recommender
Job Matching
Resume Matching
Manager & Administrator Self Service Bot
Career Planning "People like me"
Knowledge Bots
Payroll Fraud Detection

Total Workforce Insights
Job Seeker Resume Ranking
Support and Productivity Bots
Job Normalization
Job Matching for Candidates
Program Office Guidance
Timesheet Anomaly Detection
Statement of Work Builder

SAP Fieldglass Live Insights
Invoice Digitization
Risk Impact Predictions
Chatbot Bookings
Computer Vision Receipts
Anomaly Detection
Chatbot Bookings
AI Invoice Processing
Automated Duty of Care
Proactive Assistant
AI Expense Approvals

Itinerary Capture
Self-Writing Expense

Procurement

Semantic Contract Repository
Self-Service Contracts
Attribute Normalization
Semantic Search
Item Normalization
Item Recommendation
Sourcing Recommendation
Sourcing Optimization

eCommerce

Ticket Intelligence
Contextual Merchandizing
Product & Offer Recommendation
Lead Intelligence
Influencer Map & Deal Finder
Multi-Touch Customer Attribution
Customer Retention
Intelligent Customer Experience Suite

Supply Chain

Predictive & Prescriptive Maintenance
Demand Sensing
Predictive Engineering Insights
Predictive Quality Management
Advanced Forecast Accuracy
Supply Chain Segmentation
Smart Worker Enablement
Predictive Overall Equipment Effectiveness

Finance

Contract Consumption
Stock in Transit
SAP Tax Compliance Smart Automation
Cash Application
Sales Performance Prediction
Payment Block – Cash Discount at Risk
Smart Alerts for Real Spend and P&L Analysis
Demand-Driven Replenishment Adjustment

protiviti®
Face the Future with Confidence

KEY CONSIDERATIONS FOR S/4 SECURITY

Kyle Wechsler, Director – Protiviti

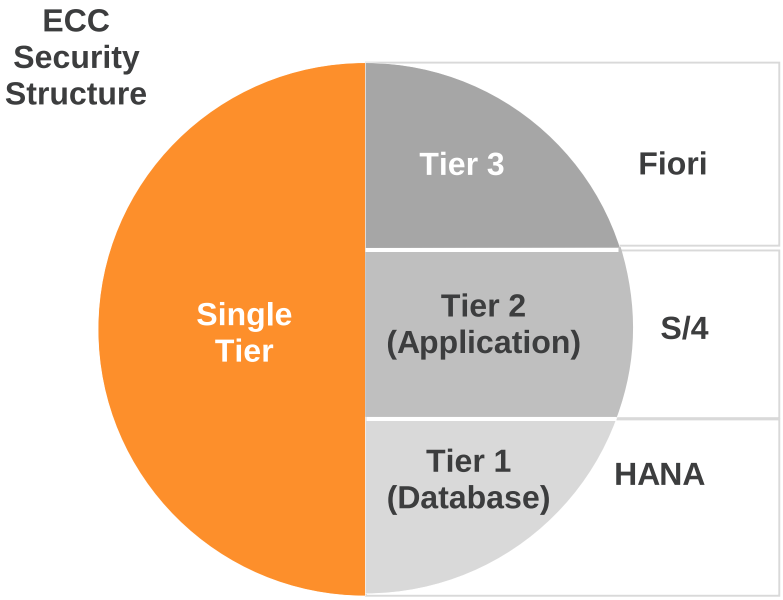
Protiviti Perspective provided by Nikhil K., New Delhi

S/4HANA SECURITY OVERVIEW

How does S/4HANA tiered approach impact your security design?

- Security architecture now encompasses three tiers, rather than prior focus on only the application layer.
- With the use of Fiori, users can access business transactions and data through apps in the Fiori Launchpad. There are thousands of Fiori apps available, and the number is growing with each new release.
- End-user access design is focused on the combination of Fiori and S/4HANA application security.
- Fiori and custom BI solutions originally required end-users to have direct access to the HANA database; however, with the introduction of new technologies such as Fiori 2.0 and S4/HANA 1709, reporting can now be achieved without granting direct access to the DB (e.g., CDS (Core Data Services) Views, AFO (Analysis for Office), etc.).

New Security Architecture



S/4HANA – WHAT IS IMPACTED?

S/4 simplification has consolidated transactions and impacted the role build structure bringing new complexities to security design. To mitigate data access risks, organizations must evaluate their system's internal control design and effectiveness, handle access to mobility requirements, and develop a security architecture that reduces risks of granting inappropriate access across S/4HANA.

	Core Layer Differences between ECC and S/4HANA	Security Impact	Audit Considerations
Application	• Legacy transactions have been consolidated and simplified • Hundreds of **new transactions** have been introduced • Traditional Customer/Vendor master data management has been replaced by the centralized Business Partner function.	• Security **roles need to be updated** for new, consolidated, and disabled transactions • Roles with Customer/Vendor access need to be revisited for potential updates • **Naming conventions** should be established/aligned across tiers • Data control language (DCL) should be implemented for ABAP-based CDS (Core Data Services) views to control access to data elements	• SoD and Sensitive Access **Ruleset will need to be updated** to include transaction and auth. object changes • Important to ensure that updated security roles are adequately tested along with functional testing procedures • Existing **security policies and procedures** (e.g. architecture, provisioning, etc.) should be updated to reflect the new security structure
Fiori	• S/4HANA allows for a more friendly and mobile user interaction • **Consolidation of multiple transactions into single Fiori applications**	• **New RFC roles** are needed to integrate S/4 and Fiori • **Frontend roles** are needed for access to business catalogs, OData Services and additional start authorizations • **Backend roles** are defined in S/4 with Odata Services in addition to traditional ABAP authorizations	• Access to Fiori apps requires a user account and access should be **restricted to the appropriate tiles** based on user roles • RFC connections should be configured to not accept expired passwords • Security needs to be assessed in all three layers: Fiori, S/4 and HANA

SAP HANA PRIVILEGES

SQL (Object) Privileges

Manage and control a user’s ability to SELECT, UPDATE, EXECUTE, DELETE SQL database objects within an SAP HANA schema. You can secure individual objects or the entire schema.

System Privileges

Govern a user’s ability to perform specific administrative or development tasks.

Package Privileges

Allow users access to view, manage, delete items in the package repository of SAP HANA. E.g., information views and repository roles are stored in this area and XS Engine code is also stored here.

Application Privileges

Privileges used by applications hosted in the SAP HANA XS application server.

Analytic Privileges

Govern a user’s ability to access information views and data within the view.

Privileges on Users

Allow the assigned user to debug another user’s SQL Script code within their session.

SECURITY REDESIGN PRIOR TO S/4HANA MIGRATION

Pros

1. **Reduce risk exposure -** rather than persistent sensitive access, segregation of duties, or excessive access issues
2. **Reduce burden on end users**
   - Prioritize security now
   - New S/4HANA functionality to be implemented separately (e.g. Fiori)
3. **Prepare for S/4HANA** during the redesign
   - Define business processes, identify role owners
4. **Leverage legacy user mapping**
   - Minimize user mapping efforts by utilizing legacy transaction usage
5. **Identify mitigating controls** for authorized conflicts
6. **Leverage redesigned roles** for your S/4HANA implementation (dependence on S/4HANA release)
   - Minimize gap analysis (ex. obsolete transactions, new t-codes)

Cons

1. **Need to reassess** 15-20% of redesign based on new S/4HANA functionality
   - New t-codes
   - New Fiori Requirements
   - Access requirements (if any) for HANA DB reporting
2. Not all redesigned roles will be **S/4HANA ready**
3. Business processes may change after moving to S/4HANA and may cause **re-work in role redesign**
4. **Governance processes** may need to be readdressed if S/4HANA is not considered as part of standards (e.g. role naming conventions, GRC processes)

ROADMAP & HISTORY OF ACCESS CONTROL

The GRC journey of where organizations have started, progressed to, and are going:

Early days of GRC

Quick Wins (Ad-hoc / Repeatable)

- Implementation of GRC 5.3
- Audit is the primary driver
- Implemented SOD monitoring & firefighter
- Monitored ECC primarily
- Ad-hoc SOD reporting by IT or audit teams

Maturity

People, Process, Tool Maturity

Enhanced Governance (Defined and Manage)

- Utilization of Access Control 10
- Progresses from Audit to CFO/Management as driver to improve compliance and efficiency
- Manage SAP user provisioning using access request management (ARM)
- Embedded SOD checks into provisioning
- Defined / documented governance
- Improved use of mitigating controls

Maturity

Automated, Intelligent, Optimized Risk View

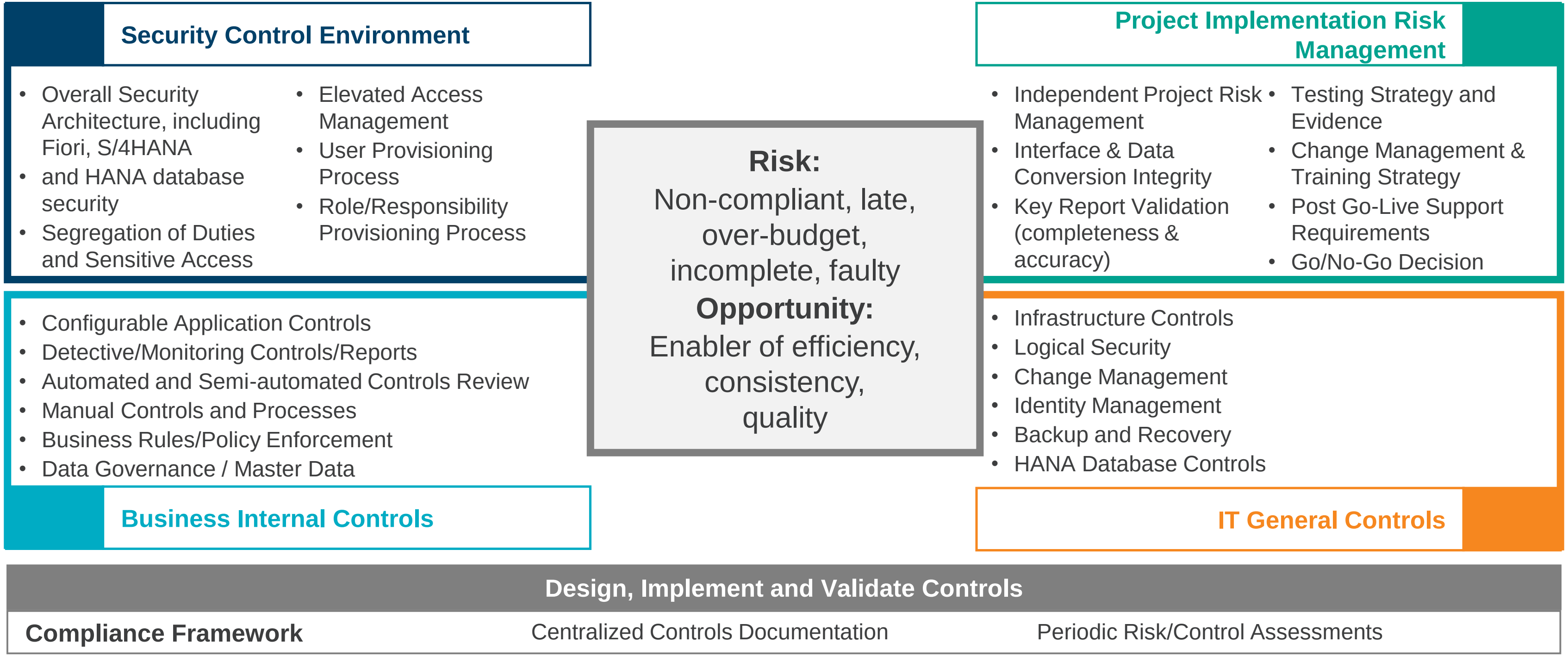
Integrated Governance (Optimized)

- Latest version of Access Control
- Integrated teams between Management, Audit, and 3rd Party Vendors
- Expand GRC connectivity (SAP, non-SAP, and cloud applications)
- Visibility of cross-system SOD risks
- Continuous monitoring using Greenlight Access Violation Management
- Automated processes with PC, RPA & IAM

Maturity

SAP RISK UNIVERSE FRAMEWORK

The objectives of the risk and compliance effort during an implementation include both monitoring implementation risk and optimizing use of the software to improve the control environment, enhance operations, and reduce compliance costs through automation of manual controls. From our understanding, we have highlighted below the items you want to discuss.



Security Control Environment

- Overall Security Architecture, including Fiori, S/4HANA
- and HANA database security
- Segregation of Duties and Sensitive Access
- Elevated Access Management
- User Provisioning Process
- Role/Responsibility Provisioning Process

Project Implementation Risk Management

- Independent Project Risk Management
- Interface & Data Conversion Integrity
- Key Report Validation (completeness & accuracy)
- Testing Strategy and Evidence
- Change Management & Training Strategy
- Post Go-Live Support Requirements
- Go/No-Go Decision

Risk:
Non-compliant, late, over-budget, incomplete, faulty
Opportunity:
Enabler of efficiency, consistency, quality

- Configurable Application Controls
- Detective/Monitoring Controls/Reports
- Automated and Semi-automated Controls Review
- Manual Controls and Processes
- Business Rules/Policy Enforcement
- Data Governance / Master Data

Business Internal Controls

- Infrastructure Controls
- Logical Security
- Change Management
- Identity Management
- Backup and Recovery
- HANA Database Controls

IT General Controls

Design, Implement and Validate Controls

Compliance Framework Centralized Controls Documentation Periodic Risk/Control Assessments

LESSONS LEARNED FROM S/4 SECURITY PROJECTS

1 **It’s critical that security is an integrated function with the implementation team**

- Designing SAP S/4, Fiori, and HANA security is highly integrated and easier when one team is responsible for at least the S/4 and Fiori components.

2 **Align Fiori business roles (frontend) with S/4 roles (backend) to streamline maintenance**

- Separate roles are required for frontend and backend and naming convention consistency and alignment is critical for maintenance as well as provisioning.

3 **Allow sufficient time for security testing**

- Security testing should be prioritized along with functional testing, and all integration points taken into consideration to ensure access works as designed and to minimize business disruption.

4 **Out of the box Fiori applications may need to be adjusted to meet business requirements**

- Demo early and plan for additional testing time.

5 **Be aware that SAP is moving towards functional / business language through Fiori design concepts**

- The Fiori application descriptions that correspond to the SAP transactions within the S/4 role design may not be the same. For example, SAP transaction ‘MIRO’ is defined as “Enter Incoming Invoice” within S/4 and “Create Supply Invoice Advanced” within Fiori.

LESSONS LEARNED FROM S/4 SECURITY PROJECTS

6

Consider job-based vs. task-based in your role design

- The best approach for your role design may vary depending on functional decisions as well as provisioning considerations

7

Consider how much to implement at one time

- Consider phased/pilot approaches as well as scope of functionality and security changes and impact on the organization

8

Integrate Governance as early as possible during the security design phase

- When designing security, take into account role ownership and approvals, user provisioning, etc.

WHEN DO WE NEED SAP HANA SECURITY?

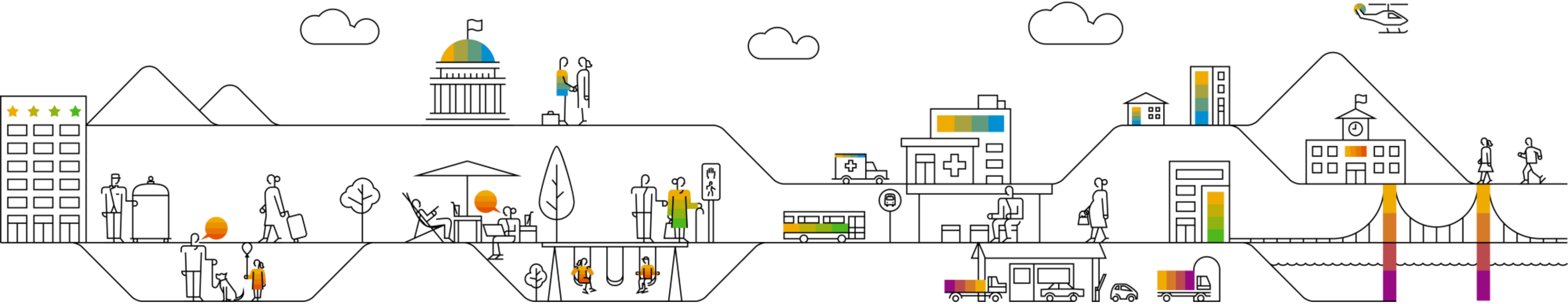
- All HANA databases require a security model, even if only to support backend administration.
- A more advanced model is required when users require direct access to the SAP HANA database.
- We need to protect the data hosted in HANA.
- Many SAP solutions require direct database access.
- Note: S/4HANA 1709 + now uses ABAP CDS views as an alternative to direct database access.

Introduction of SAP Access Control 12.0

Peter Creal, SAP, Sr. Director COE

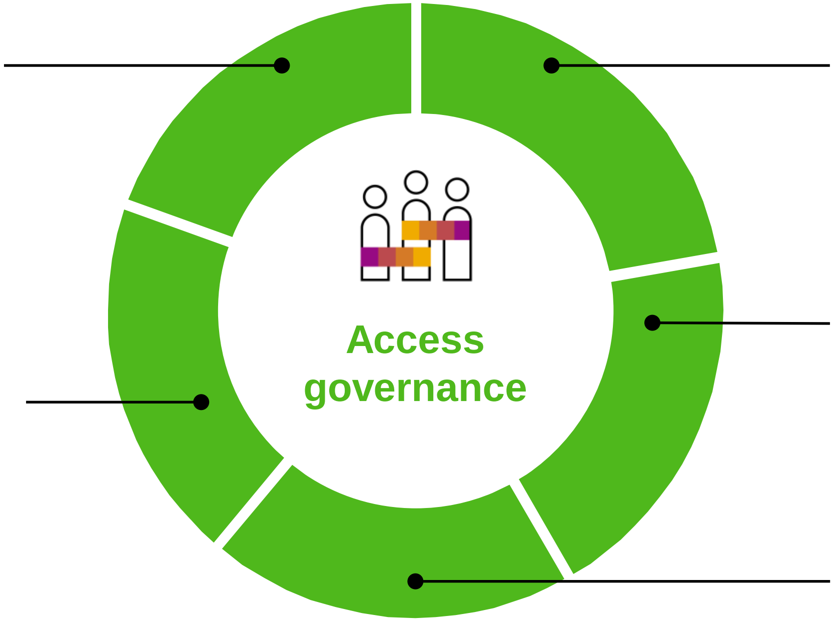
PUBLIC

Overview



SAP Access Control

Manage access risk



Access governance

Monitor privileges
Monitor emergency access and transaction usage

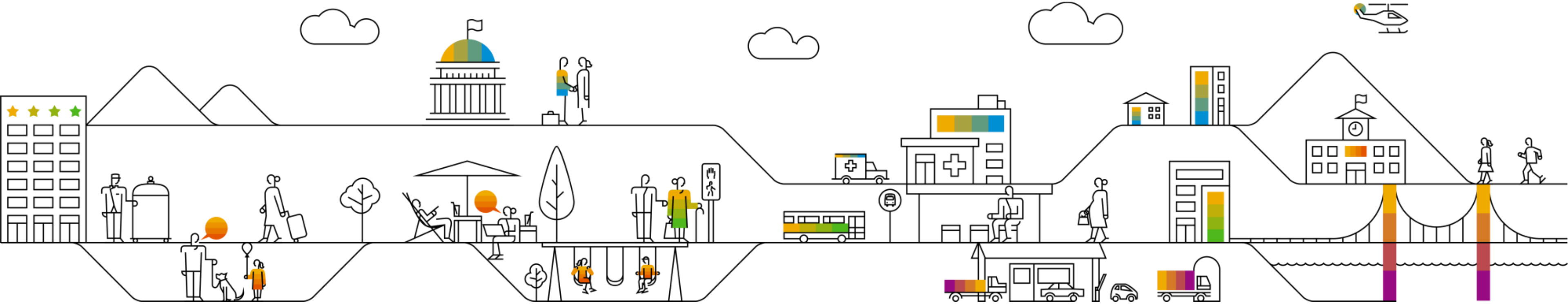
Certify authorizations
Certify that access assignments are still warranted

Analyze risk
Find and remediate segregation of duties and critical access violations

Provision users
Automate access administration for enterprise applications

Maintain roles
Define and maintain roles in business terms

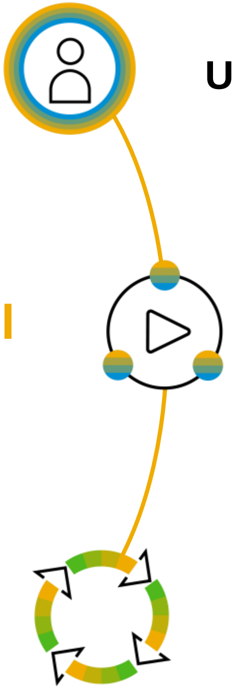
What’s New in SAP Access Control



What’s new in SAP Access Control

Themes

SAP Access Control



Usability

Integration

Process

What’s new in SAP Access Control

Usability

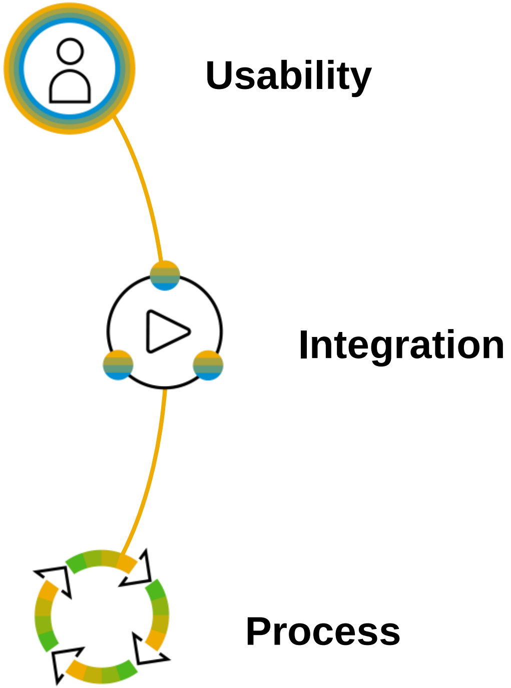
- Persona-based launchpad that simplifies navigation
- Overview page to visualize key metrics for gain greater insight

Integration

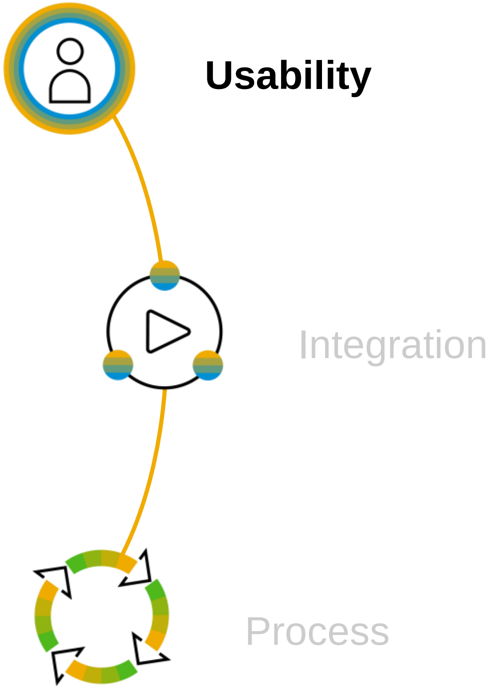
- Support cloud applications via SAP Cloud Identity Access Governance software
- End-to-end integration with SAP SuccessFactors solutions
- Access risk analysis for SAP Fiori apps in SAP S/4HANA (on premise)
- Emergency access management for SAP HANA database
- SAP Identity Management component for centralized provisioning and business-role management
- SAP SuccessFactors Employee Central Payroll solution

Process optimization

- User access review job optimization
- Repository sync optimization
- Optimized LDAP sync
- Mass role methodology update: ability to reapply methodology for multiple roles at one time
- Simplified firefighter owner and controller maintenance



Usability

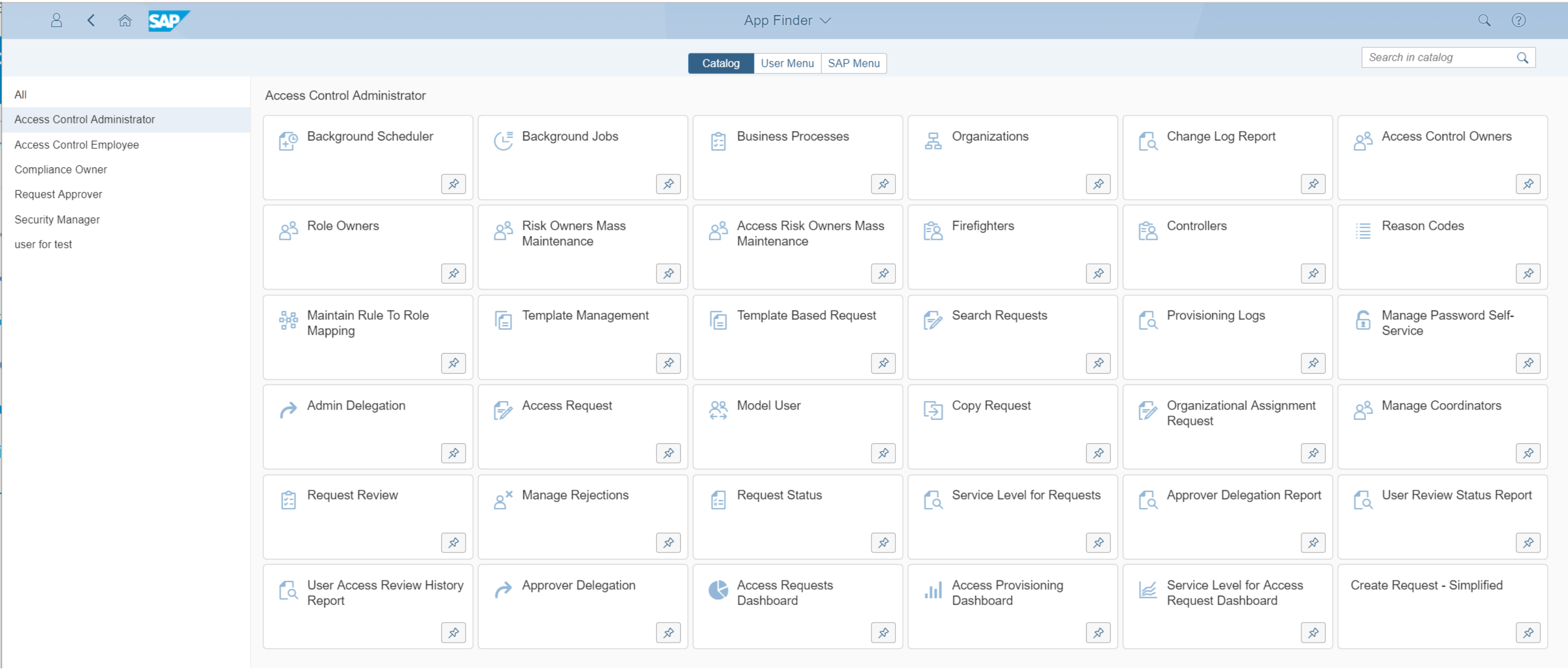


Usability

Integration

Process

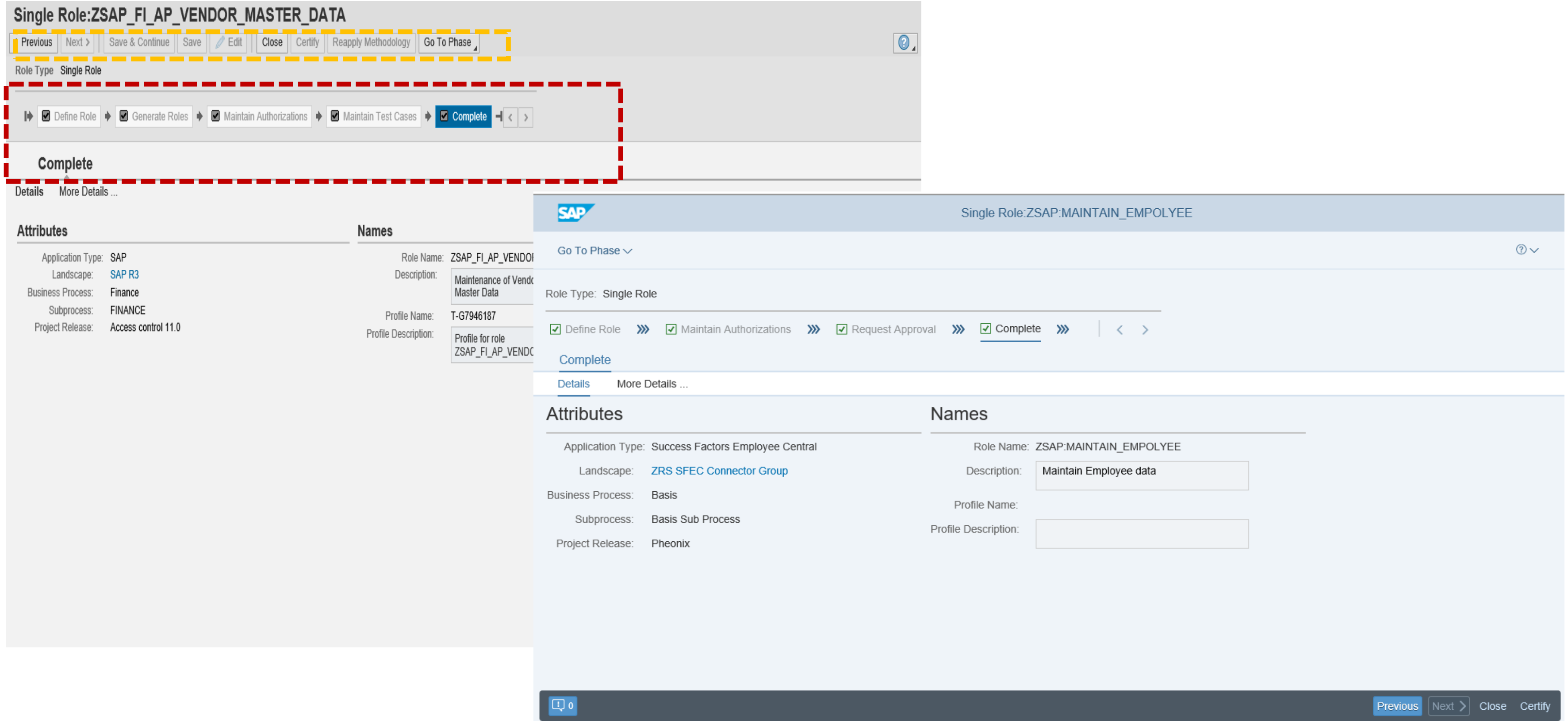
Usability: persona-based navigation simplifies navigation



Access Control Administrator

Background Scheduler	Background Jobs	Business Processes	Organizations	Change Log Report	Access Control Owners
Role Owners	Risk Owners Mass Maintenance	Access Risk Owners Mass Maintenance	Firefighters	Controllers	Reason Codes
Maintain Rule To Role Mapping	Template Management	Template Based Request	Search Requests	Provisioning Logs	Manage Password Self-Service
Admin Delegation	Access Request	Model User	Copy Request	Organizational Assignment Request	Manage Coordinators
Request Review	Manage Rejections	Request Status	Service Level for Requests	Approver Delegation Report	User Review Status Report
User Access Review History Report	Approver Delegation	Access Requests Dashboard	Access Provisioning Dashboard	Service Level for Access Request Dashboard	Create Request - Simplified

Usability: SAP Fiori user experience–like example



Single Role:ZSAP_FI_AP_VENDOR_MASTER_DATA

Role Type Single Role

Complete

Attributes

Application Type: SAP
Landscape: SAP R3
Business Process: Finance
Subprocess: FINANCE
Project Release: Access control 11.0

Names

Role Name: ZSAP_FI_AP_VENDOI
Description: Maintenance of Vendo Master Data
Profile Name: T-G7946187
Profile Description: Profile for role ZSAP_FI_AP_VENDO

Single Role:ZSAP:MAINTAIN_EMPOLYEE

Role Type: Single Role

Complete

Attributes

Application Type: Success Factors Employee Central
Landscape: ZRS SFEC Connector Group
Business Process: Basis
Subprocess: Basis Sub Process
Project Release: Pheonix

Names

Role Name: ZSAP:MAINTAIN_EMPOLYEE
Description: Maintain Employee data
Profile Name:
Profile Description:

New Reporting and Dashboards

Updated in real time – Overview Pages

- Improved usability
- Visualization driven
- Continuous real time updates
- Flexible and customizable
- New reports -

❑ Users Provisioned

❑ Active Approver Delegations

❑ User Access Review Status

❑ User Access Review History

❑ Roles by Type

❑ Roles by Generation Date

❑ Roles by Current Phase

❑ Count Authorizations in Roles

❑ Role Relationship Reports

❑ Usage Reports

❑ Access Requests by Status

❑ Access Requests by Type

❑ Requests by Due Date

❑ Service Level Violations

❑ Roles Provisioned

❑ Users with Access Risks

❑ User Access Risks History

❑ Roles with Access Risks

❑ Role Access Risks History

❑ Business Processes with Access Risks

❑ Access Risk Occurrences

❑ Alerts

❑ Active Mitigation Controls

❑ Mitigation Control Usage

❑ Risk Analysis Reports

❑ Other Reports

❑ Firefighter Activity

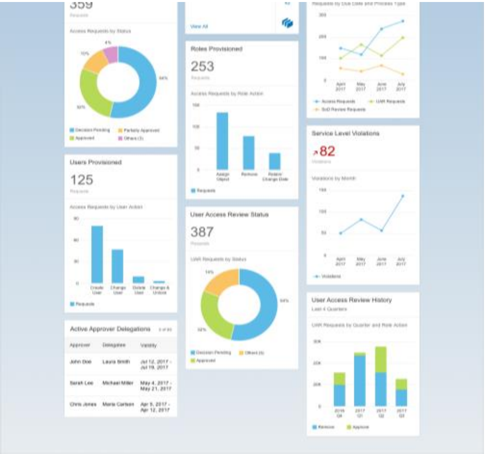
❑ Firefighter Usage by System

❑ Firefighter Log Review Status

❑ Systems with Firefighter SoD Conflicts

❑ Invalid Firefighter Assignments

❑ EAM Reports


359
Access Requests by Status
Roles Provisioned
253
Users Provisioned
125
User Access Review Status
387
Service Level Violations
82
Active Approver Delegations
User Access Review History

359
Access Requests by Status
Roles Provisioned
253
Users Provisioned
125
User Access Review Status
387
Service Level Violations
82
Active Approver Delegations
User Access Review History

Integration

Usability

Integration

Process

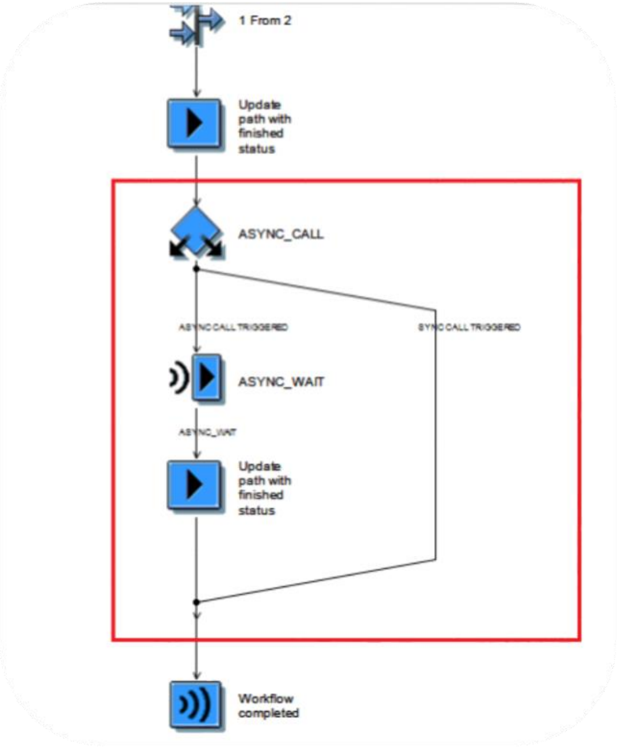
Integration: cloud applications

1. SAP Access Control → on-premise applications
2. SAP Cloud Identity Access Governance → cloud applications
3. Cloud SAP Cloud Identity Access Governance bridge sync (SAP Access Control → SAP Cloud Identity Access Governance)
   a) Access risk library
   b) Repository data
   c) Mitigation controls and mitigation (user + access risk + mitigation control + monitor)
4. SAP Access Control access request and access analysis simulation (SAP Access Control → SAP Cloud Identity Access Governance)
   a) Simulation during access request process → SAP Cloud Identity Access Governance access analysis service
   b) Mitigation in access request temporary (control look up → SAP Cloud Identity Access Governance)
   c) Persistent mitigation after approval process (SAP Access Control workflow → SAP Cloud Identity Access Governance)

Integration: SAP Identity Management

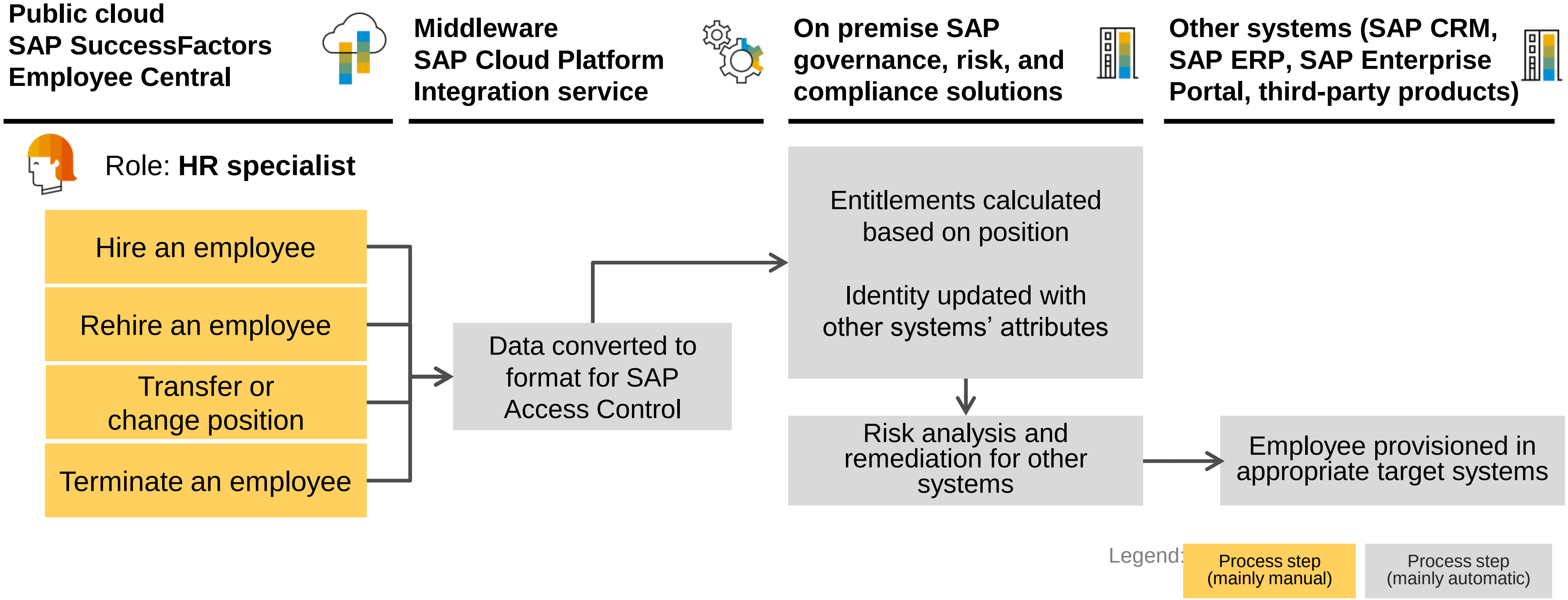
Unified business roles and provisioning scenarios with SAP Identity Management enable customers to take advantage of best practices and methodology processes from SAP governance, risk, and compliance solutions (SAP GRC).

Users can create roles and manage access via business roles for all the privileges that they need.



Integration: SAP SuccessFactors solutions

Event-driven employee lifecycle management



Public cloud
SAP SuccessFactors Employee Central

Middleware
SAP Cloud Platform Integration service

On premise SAP governance, risk, and compliance solutions

Other systems (SAP CRM, SAP ERP, SAP Enterprise Portal, third-party products)

Role: **HR specialist**

Hire an employee

Rehire an employee

Transfer or change position

Terminate an employee

Data converted to format for SAP Access Control

Entitlements calculated based on position

Identity updated with other systems’ attributes

Risk analysis and remediation for other systems

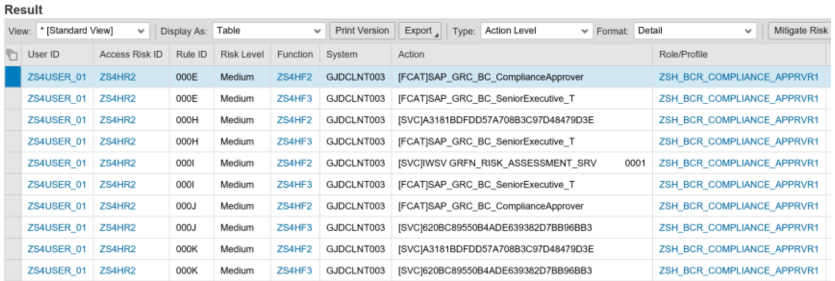
Employee provisioned in appropriate target systems

Legend: Process step (mainly manual) | Process step (mainly automatic)

Integration: Access analysis for SAP Fiori apps and SAP S/4HANA (on premise)

Ability to define risks with

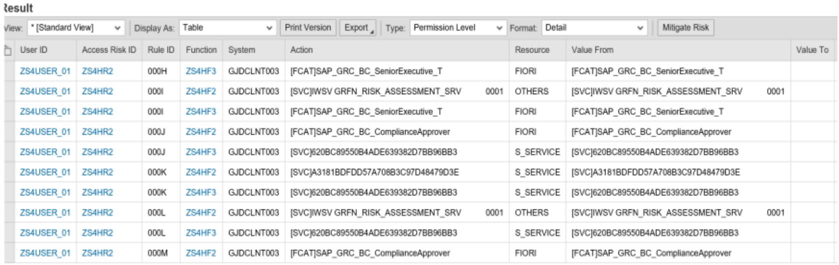
- Fiori apps, catalog, or OData service as actions
- Predefined permission mapping for SAP S/4HANA
- Ability to perform access risk analysis and report back with Fiori apps, catalogs, or OData services
- Out-of-the-box, updated risk definitions for SAP S/4HANA software rules
- Continuous update of rule set for adoption of new apps in SAP S/4HANA



Result

View: * [Standard View] | Display As: Table | Type: Action Level | Format: Detail

User ID	Access Risk ID	Rule ID	Risk Level	Function	System	Action	Role/Profile
ZS4USER_01	ZS4HR2	000E	Medium	ZS4HF2	GJDCLNT003	[FCAT]SAP_GRC_BC_ComplianceApprover	ZSH_BCR_COMPLIANCE_APPRVR1
ZS4USER_01	ZS4HR2	000E	Medium	ZS4HF3	GJDCLNT003	[FCAT]SAP_GRC_BC_SeniorExecutive_T	ZSH_BCR_COMPLIANCE_APPRVR1
ZS4USER_01	ZS4HR2	000H	Medium	ZS4HF2	GJDCLNT003	[SVC]A3181BDFDD57A708B3C97D48479D3E	ZSH_BCR_COMPLIANCE_APPRVR1
ZS4USER_01	ZS4HR2	000H	Medium	ZS4HF3	GJDCLNT003	[FCAT]SAP_GRC_BC_SeniorExecutive_T	ZSH_BCR_COMPLIANCE_APPRVR1
ZS4USER_01	ZS4HR2	000I	Medium	ZS4HF2	GJDCLNT003	[SVC]IWSV GRFN_RISK_ASSESSMENT_SRV 0001	ZSH_BCR_COMPLIANCE_APPRVR1
ZS4USER_01	ZS4HR2	000I	Medium	ZS4HF3	GJDCLNT003	[FCAT]SAP_GRC_BC_SeniorExecutive_T	ZSH_BCR_COMPLIANCE_APPRVR1
ZS4USER_01	ZS4HR2	000J	Medium	ZS4HF2	GJDCLNT003	[FCAT]SAP_GRC_BC_ComplianceApprover	ZSH_BCR_COMPLIANCE_APPRVR1
ZS4USER_01	ZS4HR2	000J	Medium	ZS4HF3	GJDCLNT003	[SVC]620BC89550B4ADE639382D7BB96BB3	ZSH_BCR_COMPLIANCE_APPRVR1
ZS4USER_01	ZS4HR2	000K	Medium	ZS4HF2	GJDCLNT003	[SVC]A3181BDFDD57A708B3C97D48479D3E	ZSH_BCR_COMPLIANCE_APPRVR1
ZS4USER_01	ZS4HR2	000K	Medium	ZS4HF3	GJDCLNT003	[SVC]620BC89550B4ADE639382D7BB96BB3	ZSH_BCR_COMPLIANCE_APPRVR1



Result

View: * [Standard View] | Display As: Table | Type: Permission Level | Format: Detail

User ID	Access Risk ID	Rule ID	Function	System	Action	Resource	Value From	Value To
ZS4USER_01	ZS4HR2	000H	ZS4HF3	GJDCLNT003	[FCAT]SAP_GRC_BC_SeniorExecutive_T	FIORI	[FCAT]SAP_GRC_BC_SeniorExecutive_T	
ZS4USER_01	ZS4HR2	000I	ZS4HF2	GJDCLNT003	[SVC]IWSV GRFN_RISK_ASSESSMENT_SRV 0001	OTHERS	[SVC]IWSV GRFN_RISK_ASSESSMENT_SRV 0001	
ZS4USER_01	ZS4HR2	000I	ZS4HF3	GJDCLNT003	[FCAT]SAP_GRC_BC_SeniorExecutive_T	FIORI	[FCAT]SAP_GRC_BC_SeniorExecutive_T	
ZS4USER_01	ZS4HR2	000J	ZS4HF2	GJDCLNT003	[FCAT]SAP_GRC_BC_ComplianceApprover	FIORI	[FCAT]SAP_GRC_BC_ComplianceApprover	
ZS4USER_01	ZS4HR2	000J	ZS4HF3	GJDCLNT003	[SVC]620BC89550B4ADE639382D7BB96BB3	S_SERVICE	[SVC]620BC89550B4ADE639382D7BB96BB3	
ZS4USER_01	ZS4HR2	000K	ZS4HF2	GJDCLNT003	[SVC]A3181BDFDD57A708B3C97D48479D3E	S_SERVICE	[SVC]A3181BDFDD57A708B3C97D48479D3E	
ZS4USER_01	ZS4HR2	000K	ZS4HF3	GJDCLNT003	[SVC]620BC89550B4ADE639382D7BB96BB3	S_SERVICE	[SVC]620BC89550B4ADE639382D7BB96BB3	
ZS4USER_01	ZS4HR2	000L	ZS4HF2	GJDCLNT003	[SVC]IWSV GRFN_RISK_ASSESSMENT_SRV 0001	OTHERS	[SVC]IWSV GRFN_RISK_ASSESSMENT_SRV 0001	
ZS4USER_01	ZS4HR2	000L	ZS4HF3	GJDCLNT003	[SVC]620BC89550B4ADE639382D7BB96BB3	S_SERVICE	[SVC]620BC89550B4ADE639382D7BB96BB3	
ZS4USER_01	ZS4HR2	000M	ZS4HF2	GJDCLNT003	[FCAT]SAP_GRC_BC_ComplianceApprover	FIORI	[FCAT]SAP_GRC_BC_ComplianceApprover	

Integration: Firefighter for SAP HANA database

Key benefits

- Extends emergency access management for SAP HANA database
- Provides end-to-end emergency access and transaction log collection for auditability
- Enables customer to manage critical actions on SAP HANA database, especially when it comes to SAP HANA as the analytical platform
- Reduces additional training through simple seamless integration of SAP HANA within standard emergency access management tooling

Functions

- Simple SAP HANA connection
- Integration with emergency access management launchpad
- Firefighter ID role per SAP HANA database connector
- Customizable audit policies to get focused traction log
- Integrated log collection with common framework

Integration: SAP Identity Management

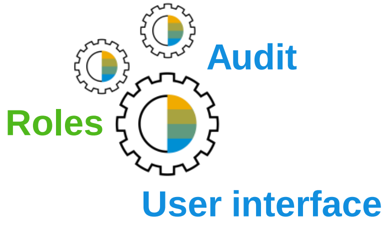
SAP Identity Management and SAP Access Control as an integrated solution for identity and access governance

- Unified business-role management
- SAP Access Control 10.1 and higher as the solution to model business roles and implement access governance
- SAP Identity Management as the solution to provision identities and access to all connected systems

Solution

- SAP Access Control imports privileges of business applications from SAP Identity Management.
- Role administrator defines business roles in SAP Access Control based on the imported privileges.
- SAP Identity Management loads business roles from SAP governance, risk, and compliance solutions, making them available for provisioning.
- Models are continuously kept in sync.
- User and assignments are provisioned.

SAP Access Control



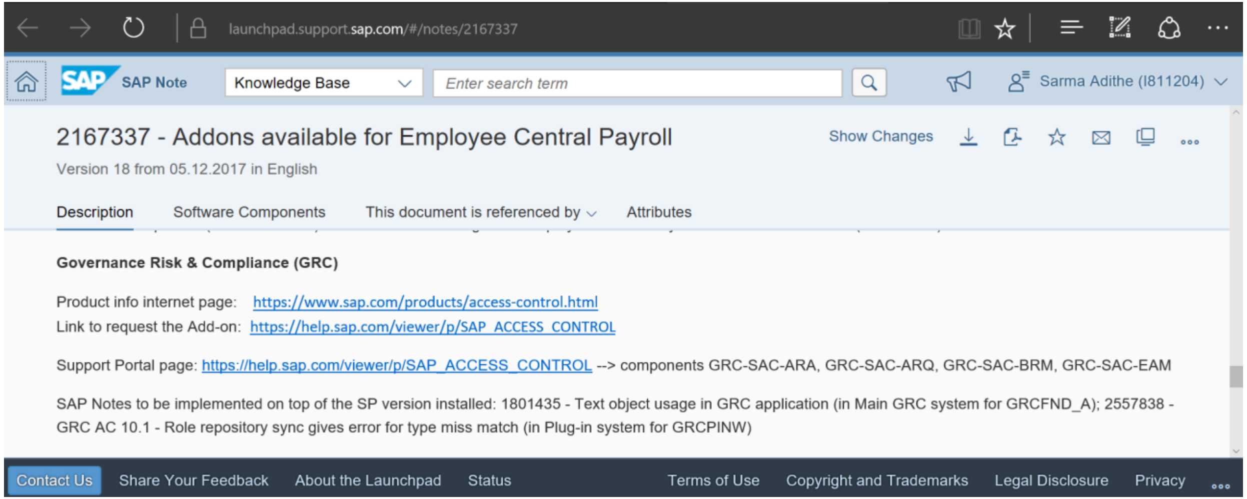
SAP Identity Management

Integration: SAP SuccessFactors Employee Central Payroll

Starting from SAP Access Control 10.1 SP19

Note: [2167337 – Add-ons available for SAP SuccessFactors Employee Central Payroll]()

Customers can connect their SAP SuccessFactors Employee Central Payroll solution to on-premise SAP Access Control



2167337 - Addons available for Employee Central Payroll

Version 18 from 05.12.2017 in English

Governance Risk & Compliance (GRC)

Product info internet page: https://www.sap.com/products/access-control.html
Link to request the Add-on: https://help.sap.com/viewer/p/SAP_ACCESS_CONTROL

Support Portal page: https://help.sap.com/viewer/p/SAP_ACCESS_CONTROL --> components GRC-SAC-ARA, GRC-SAC-ARQ, GRC-SAC-BRM, GRC-SAC-EAM

SAP Notes to be implemented on top of the SP version installed: 1801435 - Text object usage in GRC application (in Main GRC system for GRCFND_A); 2557838 - GRC AC 10.1 - Role repository sync gives error for type miss match (in Plug-in system for GRCPINW)

Process

Usability

Integration

Process

Performance: user access review request generation

Optimized user access review generation for business roles

Adds new filter criteria in user access review for business role

- Business process
- Critical level
- Role sensitivity
- Functional area
- Excluded expired roles

Reading usage information is optimized to reduce overhead.

Batch processing of range data is enabled to avoid potential dumps.

Performance: repository sync optimization

Depending on the volume of data that customers have, repository synch jobs could potentially take longer. When there are dependent jobs, it is hard to manage running one over the other.

With this new solution, customers can schedule parallel jobs and dependent jobs to optimize the process.

Process

1. Create a variant with a schedule
2. Create parallel job variants with sequence and dependency
3. Schedule the number of processes to run set of parallel jobs

Performance: LDAP sync

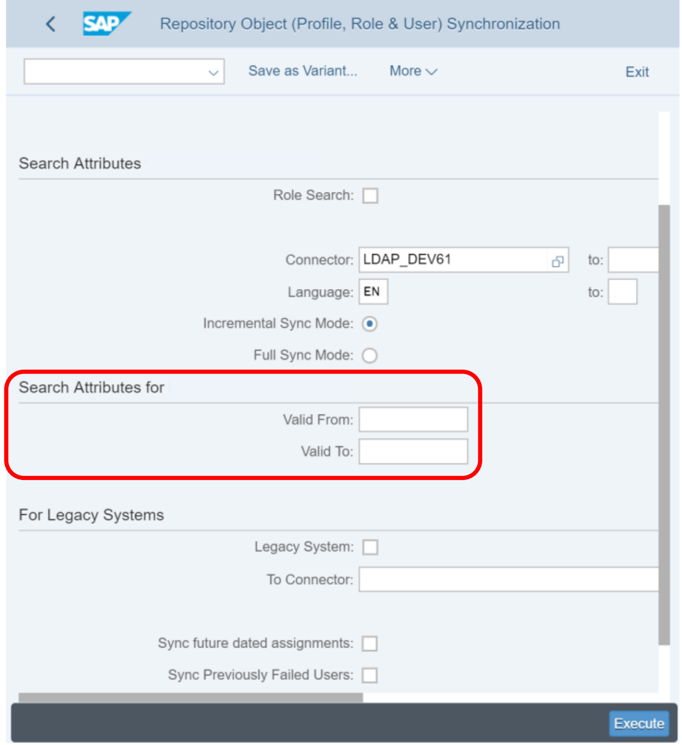
Problem

During “Repository Sync” for LDAP sync, it could take a long time for initial (full sync) if the customer has lot of historical data. The last sync date always defaults to the year 1970 at the first sync.

Depending on the volume of data, this sync may result in dumps.

Solution

We introduced a set of new parameters that can restrict the sync using a “from” date and “to” date. If left blank, the “to” date is usually taken as the current date.



Search Attributes

Role Search: □

Connector: LDAP_DEV61 to:

Language: EN to:

Incremental Sync Mode: ●

Full Sync Mode: ○

Search Attributes for

Valid From:

Valid To:

For Legacy Systems

Legacy System: □

To Connector:

Sync future dated assignments: □

Sync Previously Failed Users: □

Process optimization: mass-role methodology update

Mass-role methodology update: ability to perform reapply methodology for multiple roles at a time

This functionality will enable you to select multiple roles at a time and update the methodology process. Default methodology will be considered to update the roles, and the background job will be scheduled to update the methodology process.

Process optimization: firefighter owner and controller maintenance

Current owner and controller maintenance

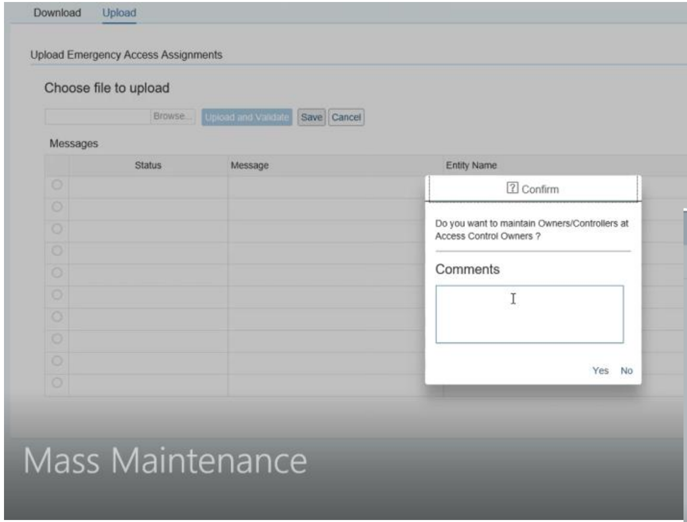
- User must be maintained first by the SAP Access Control owner.
- Only that user can be maintained as owner or controller to FFIDs.
- This is a double maintenance process. This process is now optimized to avoid double maintenance and provide user flexibility to assign owners and controllers to FFIDs irrespective of the user maintained as the SAP Access Control owner.

Process

1. Before saving the owners and controllers assignment, user is prompted with a confirmation whether to maintain the user as access control owner.
2. If the decision is “yes,” then the assignment is saved along with user maintenance as access control owner.
3. This applies for mass maintenance as well.

Process optimization: firefighter owner controller maintenance

Owner assignment



Upload Emergency Access Assignments

Choose file to upload

Messages

Status	Message	Entity Name	Line Number

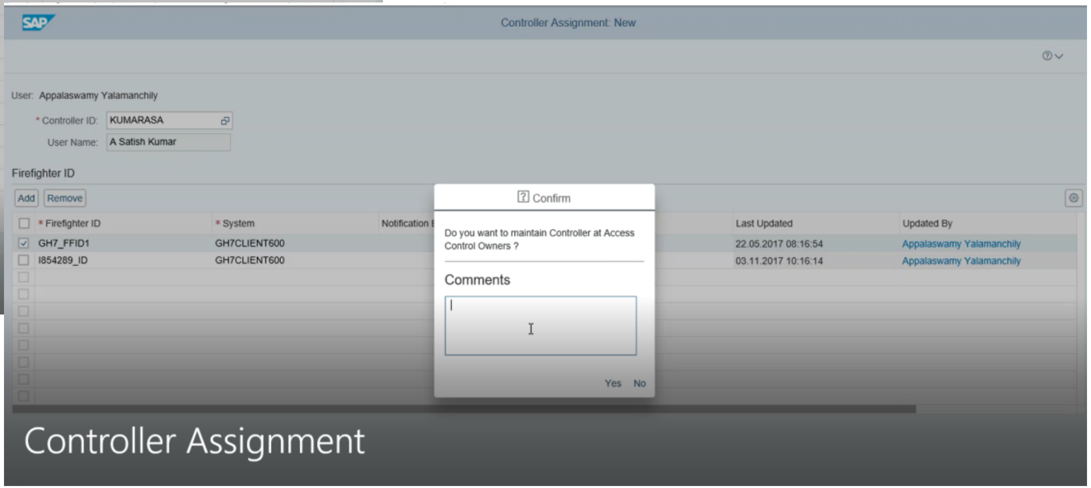
Confirm

Do you want to maintain Owners/Controllers at Access Control Owners ?

Comments

Mass Maintenance

Controller assignment



Controller Assignment: New

User: Appalaswamy Yalamanchily

* Controller ID: KUMARASA

User Name: A Satish Kumar

Firefighter ID

	* Firefighter ID	* System	Notification	Last Updated	Updated By
☑	GH7_FFID1	GH7CLIENT600		22.05.2017 08:16:54	Appalaswamy Yalamanchily
□	I854289_ID	GH7CLIENT600		03.11.2017 10:16:14	Appalaswamy Yalamanchily

Confirm

Do you want to maintain Controller at Access Control Owners ?

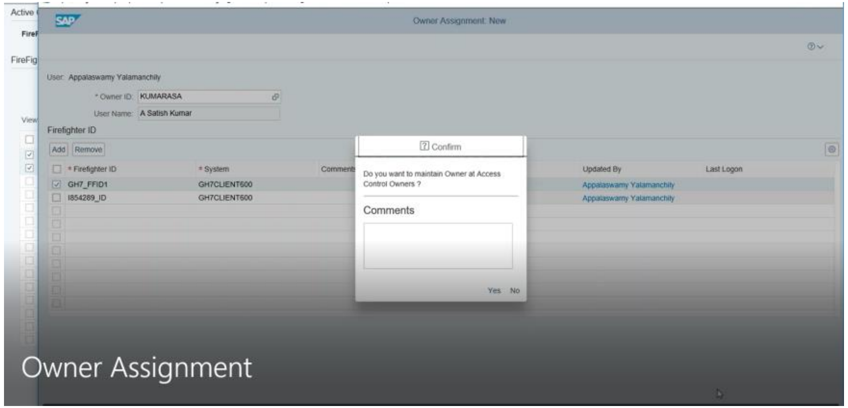
Comments

Controller Assignment

Process optimization: firefighter owner controller maintenance (continued)

Mass maintenance

During mass maintenance, if any owner or controller is not maintained as an access control owner, then the end user receives confirmation.



User: Appalaswamy Yalamanchily

* Owner ID: KUMARASA

User Name: A Satish Kumar

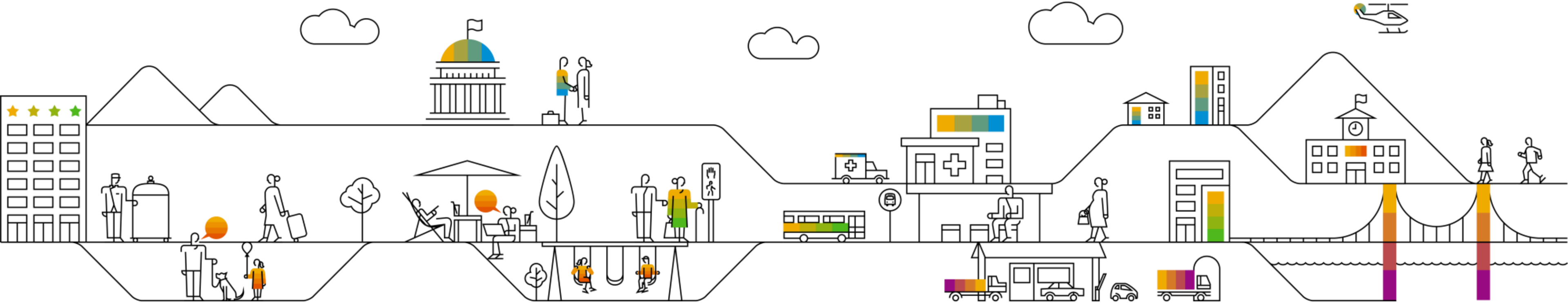
Firefighter ID

	* Firefighter ID	* System	Comments	Updated By	Last Logon
☑	GH7_FFID1	GH7CLIENT600		Appalaswamy Yalamanchily	
□	I854289_ID	GH7CLIENT600		Appalaswamy Yalamanchily	

Do you want to maintain Owner at Access Control Owners ?

Comments

Wrap-Up



Summary

- Customers get simplified navigation and improved user experience with new SAP Access Control 12.0.
- Overview pages provide insight and allow drill-down to actions to fulfill compliance needs.
- SAP Cloud Identity Access Governance complements SAP Access Control on premise.
- Integration with SAP SuccessFactors solutions simplifies access governance and automates user onboarding to business applications.
- Access governance for new authorization models like SAP S/4HANA and SAP Fiori is extended.
- Emergency access management for the SAP HANA database allows auditable administrative access to SAP HANA.
- SAP Access Control extends access governance to cloud solutions.

Overview of the SAP Cloud Identity Access Governance Offering

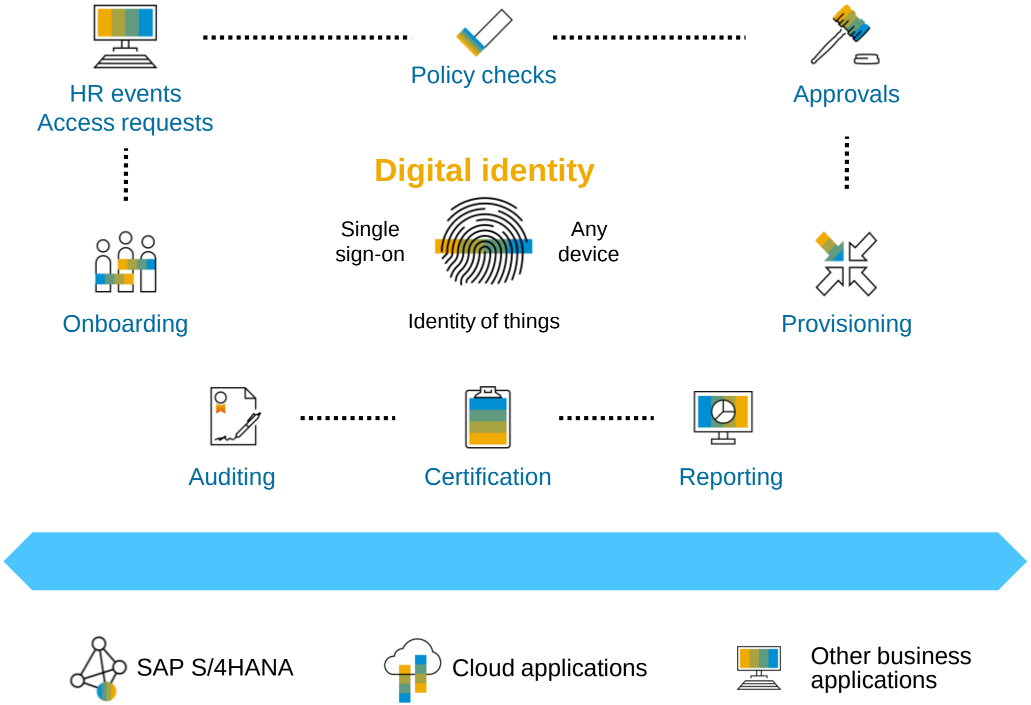
Sarma Adithe – SAP, Chief Product Owner, SAP Access Control, SAP Cloud Identity Access Governance

Access governance

Digital identity–enabled enterprise

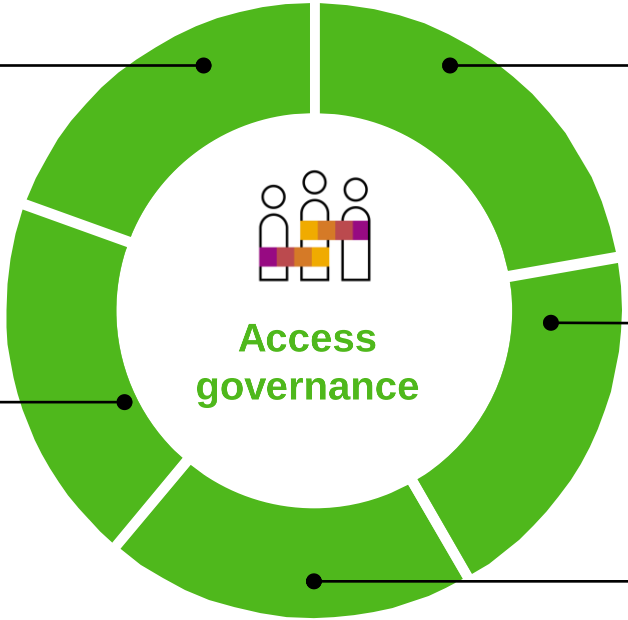
Access governance and data protection

- Reduce cost and improve security with identity management and automated provisioning
- Manage access for enterprise applications
  - – Cloud or on premise
  - – Role or attribute-based controls
- Enable greater user productivity by eliminating excessive logins with single sign-on
- Reduce audit costs by quantifying the financial impact of access risk violations
- Support and monitor critical capabilities and accounts for privileged users



SAP Cloud Identity Access Governance offering

Simple, seamless, and adaptive



Privilege access management*
Achieve account-based access, log consolidation, and review with automated log assessment for fraud

Access certification*
Review access, role, risk, and mitigation control

Access analysis
Analyze access, refine user assignments, manage controls

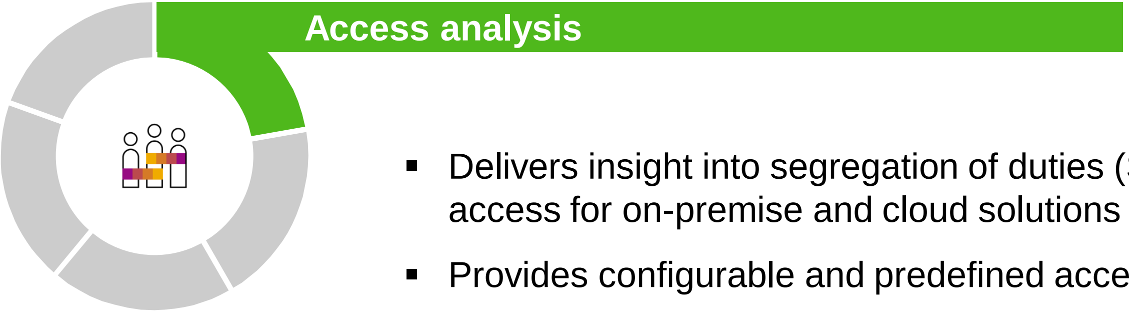
Role design
Optimize role definition and streamline governance

Access request
Optimize access, workflow, policy-based assignment, and processes

Planned 2019*

SAP Cloud Identity Access Governance, access analysis service

Analyze access, refine user assignments, manage controls

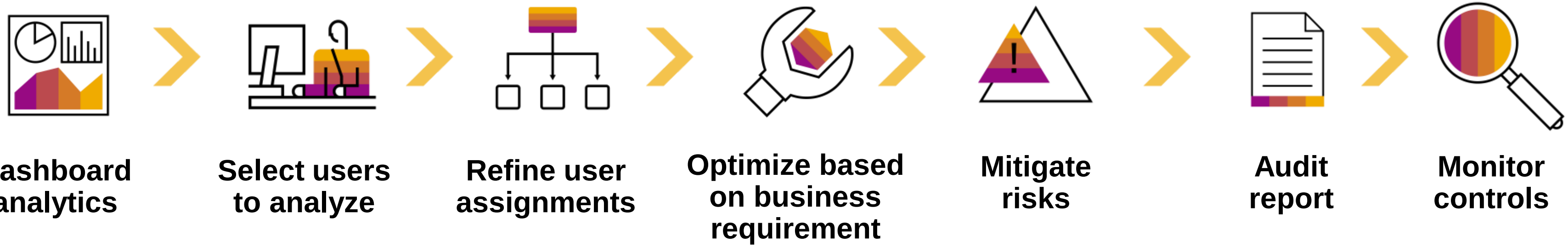


Access analysis

- Delivers insight into segregation of duties (SoD) and critical access for on-premise and cloud solutions with built-in risk scoring
- Provides configurable and predefined access policies and rules
- Enables refinement of assignments to optimize user access for security and compliance
- Allows management of controls including integrated control monitoring and testing
- Enables preconfigured audit reporting

SAP Cloud Identity Access Governance offering

Analyze access, refine user assignments, manage controls – access analysis service



Dashboard analytics

Select users to analyze

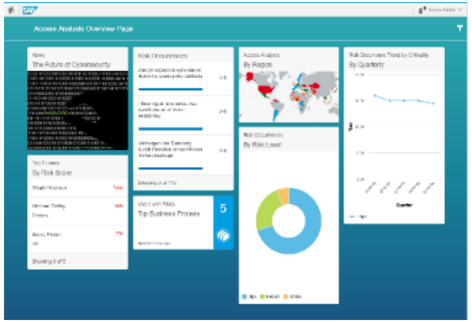
Refine user assignments

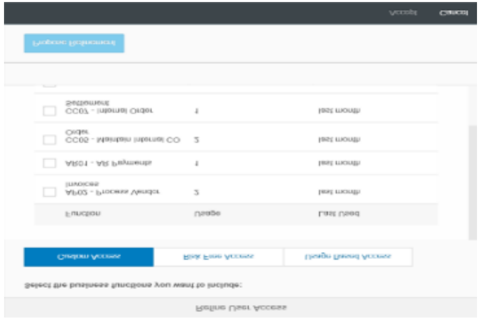
Optimize based on business requirement

Mitigate risks

Audit report

Monitor controls

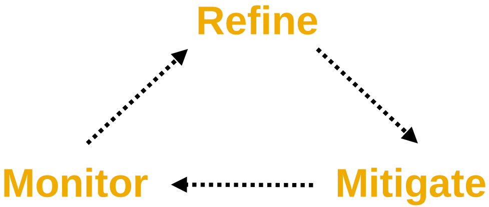




Refine User Access

Select the business functions you want to include:

Function	Usage	Last Used
AP03 - Process Vendor Invoices	3	last month
AR01 - AR Payments	1	last month
CC06 - Maintain Internal CO Order	3	last month
CC07 - Internal Order Settlement	1	last month



Refine

Mitigate

Monitor

SAP Cloud Identity Access Governance, role design service

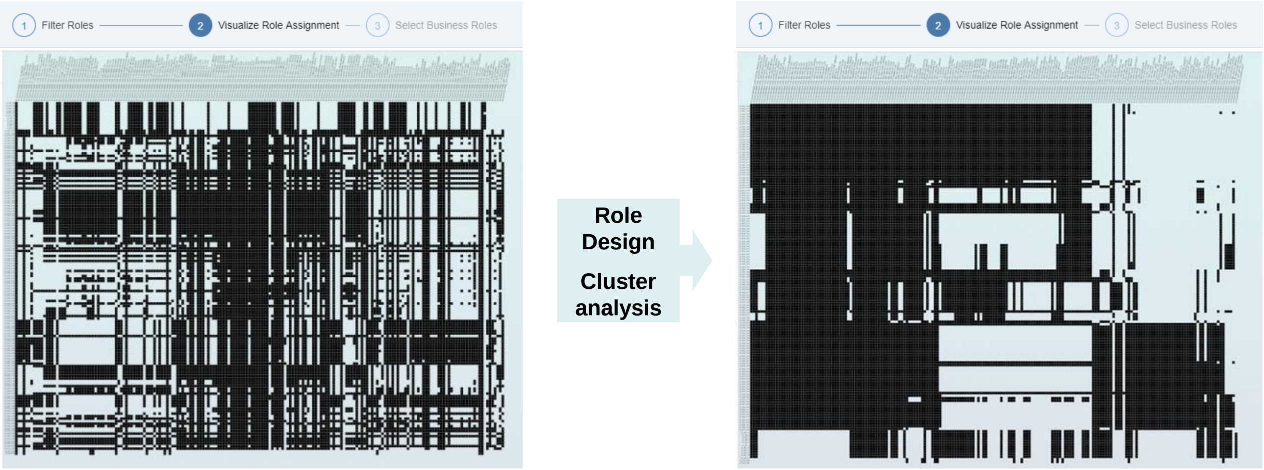
Optimize role definition and streamline governance

Role design

- SAP Fiori-based, bottoms-up business role design and role refactoring
- Ability to assure business role compliance with organizational policies
- Integrated reconciliation process to help ensure consistency of business roles
- Ability to smoothly link access analysis and role design

Bottoms-up role design

Optimize role definition and streamline governance



Role Design

Cluster analysis

- Create business roles based on existing assignments
- Add or remove roles to map functional requirements with system technical role assignments
- Reduce the number of roles required to administer access
- Create abstraction layer, reducing the need to separately administer each user, role, and system

Key benefits

Reduce the complexity of role administration

Simplify process of determining correct access assignments

Reduce the number of roles necessary to manage access

SAP Cloud Identity Access Governance offering

Optimize role definition and streamline governance – role design service

Enhanced user experience and productivity with optimized access definition

Mine roles

- Roles, privileges, and authorizations
- User access
- Usage activity

Optimize access

- Analyze mined access information
- Discover optimal granularity of authorizations

Refine access

- Propose optimal user access
- Orchestrate access for an end-to-end business process

Analyze impact

- Adjust role content to remediate risks
- Mitigate risks as applicable

Provision users

- Assign access to users
- Notify users

This is the current state of planning and may be changed by SAP at any time.

SAP Cloud Identity Access Governance, access request service

Optimize access, workflow, policy-based assignment, and processes

Access request

- Self-service access-request forms with built-in guides and data-driven filters
- Auditable access-request workflow
- Integrated, compliant user-provisioning process
- Native integration with cloud apps

Integrated provisioning for hybrid landscapes

On premise

SAP S/4HANA Cloud

SAP Ariba

SAP SuccessFactors

Microsoft Azure

SAP S/4HANA

SAP ECC

SAP Concur*

SAP Fieldglass*

SAP C/4HANA*

Cloud

- Seamless access governance across hybrid landscapes
- Automated access request approval and provisioning based on HR events
- Expanded system connectors for key business applications on-premise and cloud
- S/4 HANA native integration including rule content and support for new authorization model

Key benefits

Increased scope for provisioning across hybrid landscapes

Simplified architecture leveraging common components

Enable and govern users for processes that span multiple applications

*Planned

SAP Cloud Identity Access Governance, access certification service

Review access, role, risk, and mitigation control

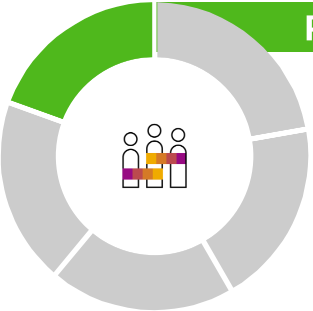
Access certification*

- Automate periodic access reviews
- Enable reviews specific to organizational needs
- Support large-scale reviews
- Manage the review process
- Access data-driven views for the review process

*Planned 2019

SAP Cloud Identity Access Governance, privilege access management service

Account-based access, log consolidation, and review with automated log assessment for fraud



Privilege access management*

- Administration of privileged user accounts
- Temporary use of elevated permissions
- Integrated session tracking
- Workflow-based activity review

*Planned 2019

SAP Cloud Identity Access Governance offering

Feature overview

Access analysis

- Delivers insight into segregation of duties (SoD) and critical access for on-premise and cloud solutions
- Provides configurable and predefined access policies and rules
- Enables refinement of assignments to optimize user access for security and compliance
- Allows management of controls including integrated control monitoring and testing
- Enables preconfigured audit reporting

Role design

- SAP Fiori-based, bottoms-up business role design and role refactoring
- Ability to assure business role compliance with organizational policies
- Integrated reconciliation process to help ensure consistency of business roles
- Ability to smoothly link access analysis and role design

Access request

- Self-service access request forms with built-in guides and data-driven filters
- Auditable access request workflow
- Integrated, compliant user provisioning process
- Native integration with cloud apps

Access certification*

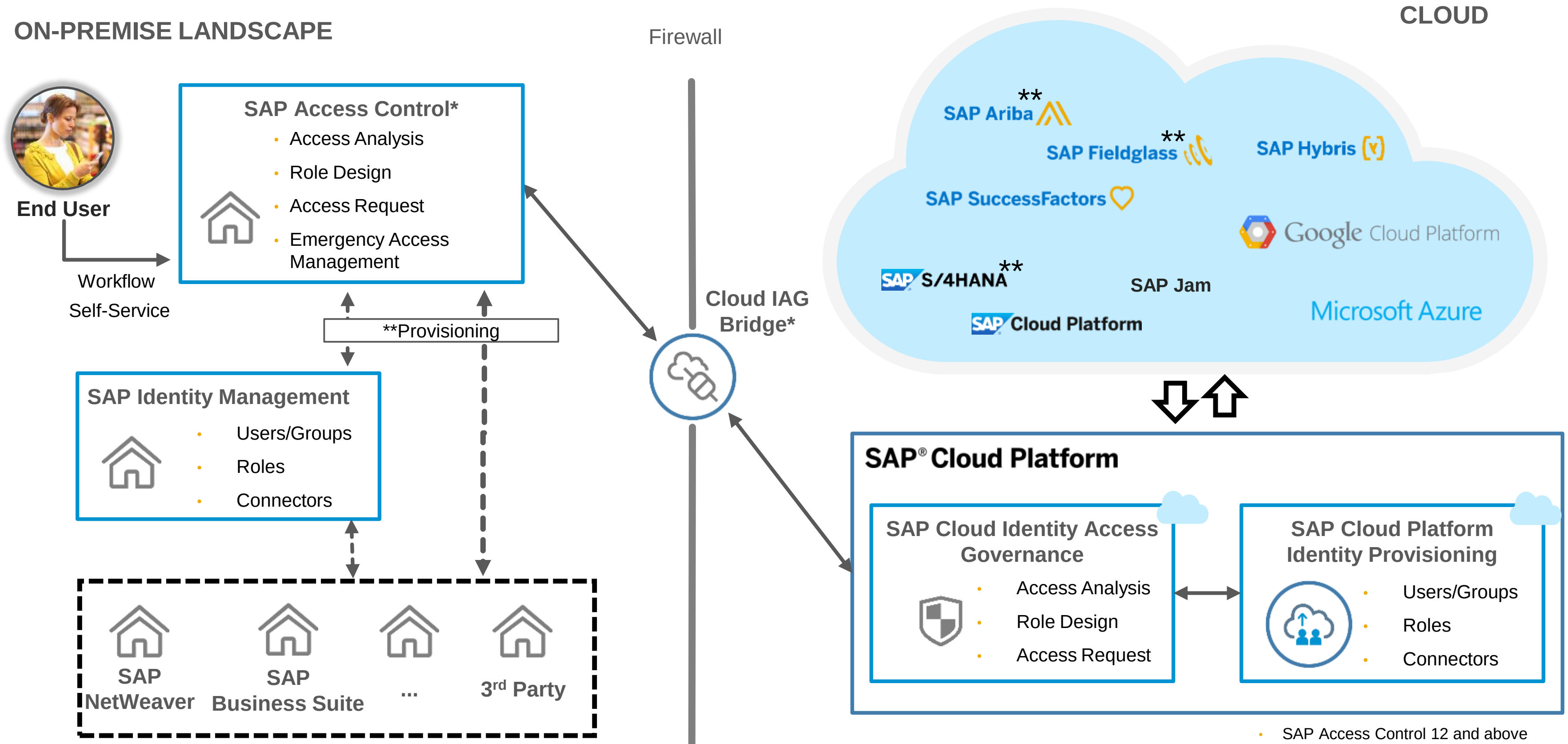
- Automate periodic access reviews
- Enable reviews specific to organizational needs
- Support large-scale reviews
- Manage the review process
- Access data-driven views for the review process

Privilege access management*

- Administration of privileged user accounts
- Temporary use of elevated permissions
- Integrated session tracking
- Workflow-based activity review

*Planned 2019

Hybrid Identity and Access Governance



ON-PREMISE LANDSCAPE

End User

Workflow

Self-Service

SAP Access Control*

- Access Analysis
- Role Design
- Access Request
- Emergency Access Management

**Provisioning

SAP Identity Management

- Users/Groups
- Roles
- Connectors

SAP NetWeaver

SAP Business Suite

...

3rd Party

Firewall

Cloud IAG Bridge*

CLOUD

SAP Ariba **

SAP Fieldglass **

SAP Hybris

SAP SuccessFactors

Google Cloud Platform

SAP S/4HANA **

SAP Jam

SAP Cloud Platform

Microsoft Azure

SAP® Cloud Platform

SAP Cloud Identity Access Governance

- Access Analysis
- Role Design
- Access Request

SAP Cloud Platform Identity Provisioning

- Users/Groups
- Roles
- Connectors

- SAP Access Control 12 and above

**Optional

WHAT’S NEW WITH GRC 12.0: THE ROAD AHEAD

Madhu Mathew, Associate Director – Protiviti

Protiviti Perspective provided by Nikhil K., New Delhi

SAP ACCESS CONTROL FUNCTIONALITY WITH S/4HANA

SAP GRC functionality has been expanded for S/4HANA, but there are new system opportunities and considerations you can take into account:

Access Risk Analysis

- Shift in architecture requires ruleset review to consider S/4HANA changes, Fiori, MDG, and other applications.
- User and Role risk analysis can be performed for the HANA database.
- Cross-system SOD risks a larger concern.

Access Request Management

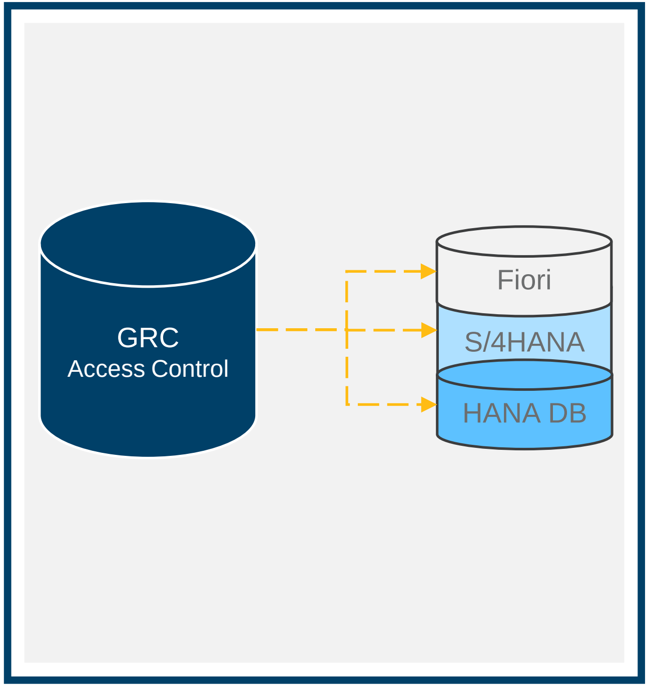
- Consider development of Enterprise Business Roles to align with identities and job roles to provision access to S/4HANA, Fiori, and other SAP applications (SuccessFactors, Ariba, etc.).
- Access requests should be an exception.
- GRC can be used to provision users, roles, and analytic privileges in SAP HANA database.

Emergency Access Management

- Firefighter access and EAM workflows are supported for S/4HANA, Fiori, and HANA.
- Centralize privilege access management for connected systems.

Business Role Management

- Role management functionality can be used for S/4HANA.
- Business Role concept is a must to ensure streamlined user experience when requesting access.



SAP S/4HANA SOD RULESET CONSIDERATIONS

Various Ruleset Options

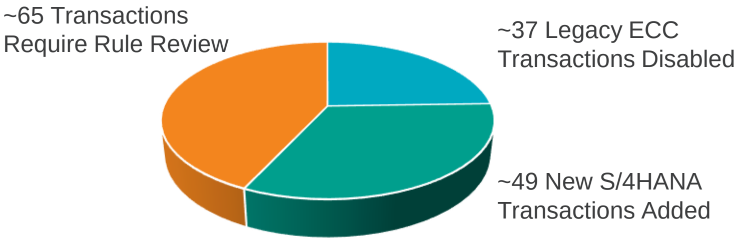
GRC ruleset updates are required to take into account the new and changed functionality in S/4HANA

- New Functionality (e.g. asset posting capabilities in central finance)
- Changed Functionality (e.g., moving master data maintenance to a business partner function)
- New or Updated Authorization Object Updates

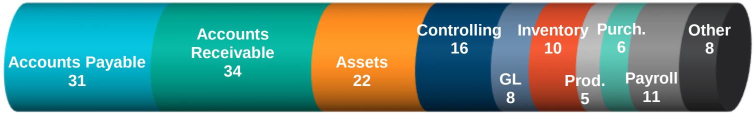
Why are SOD Ruleset Updates Necessary?

- Omitting new transactions from the SOD ruleset can drastically reduce its effectiveness in mitigating risks
- Numerous transactions were noted for removal, however our expert analysis shows that many ECC t-codes remain functional
- New Authorization Objects (e.g., Business Partner objects) have been introduced to perform key functionality such as Vendor Maintenance. Overlooking these updates could result in inaccurate SOD reports as many real risks may not appear

Ruleset Changes For S/4HANA

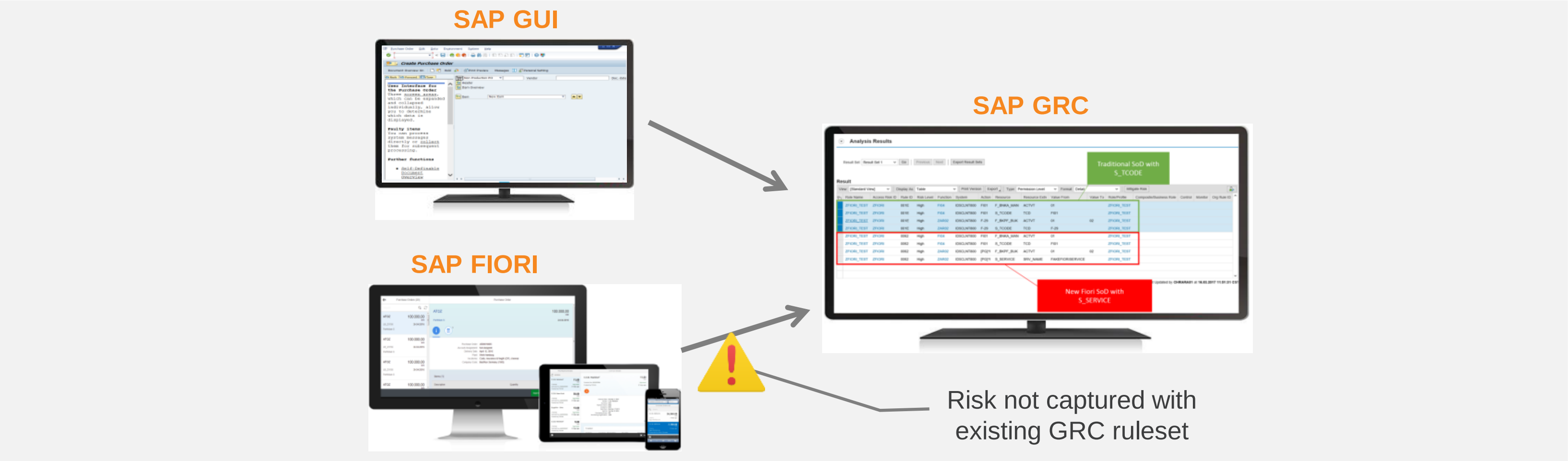


New Transactions Considered for S/4HANA SOD Ruleset



FIORI RULESET EXAMPLE

- Fiori introduces new authority checks that must be integrated into existing GRC ruleset.
  - The Fiori Application will leverage object services versus the traditional transaction code check.
  - This means the service name for the Fiori App (e.g. C_PURCHASEORDER_FS_SRV) will need to be maintained in the GRC ruleset in conjunction with the existing t-code checks.



Risk not captured with existing GRC ruleset

CONSIDER IMPLEMENTING OR UPGRADING TO GRC 12.0

AC 12.0 is going to be the latest release of SAP GRC in 2018. Several considerations may drive organizations decision to implement or to upgrade to GRC 12.0:

SAP Cloud Products

- Multiple SAP Cloud applications and have a single compliance and risk control process across all SAP applications
- Managing a single user provisioning and emergency access management process across SAP applications

Greenfield SAP Implementation

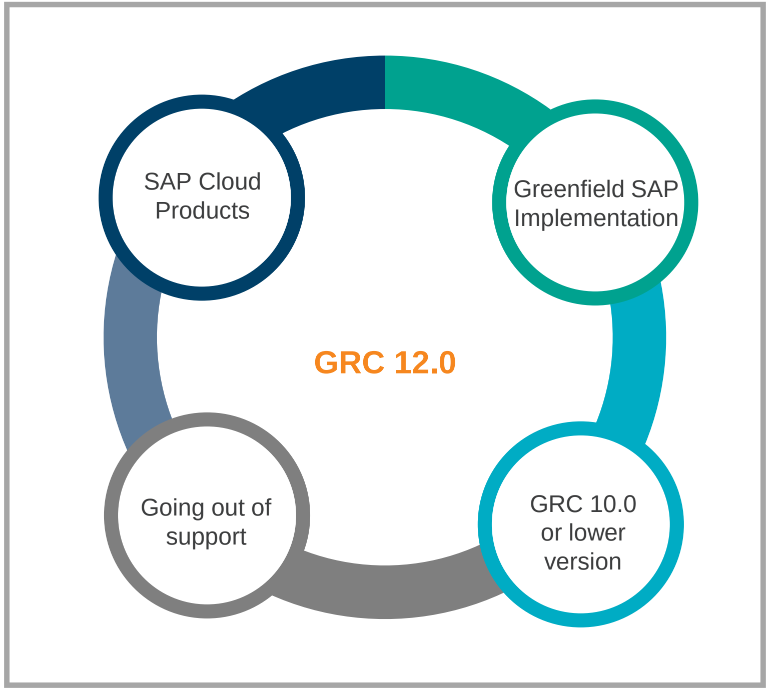
- New SAP implementation and leveraging the multiple versions of SAP products
- Monitoring and managing in a hybrid environment of on premise and cloud

GRC 10.0 or lower version

- Using AC 10.0 or 10.1 but not at the latest support packs
- Looking to mature governance using recent functional updates in AC

Going out of support

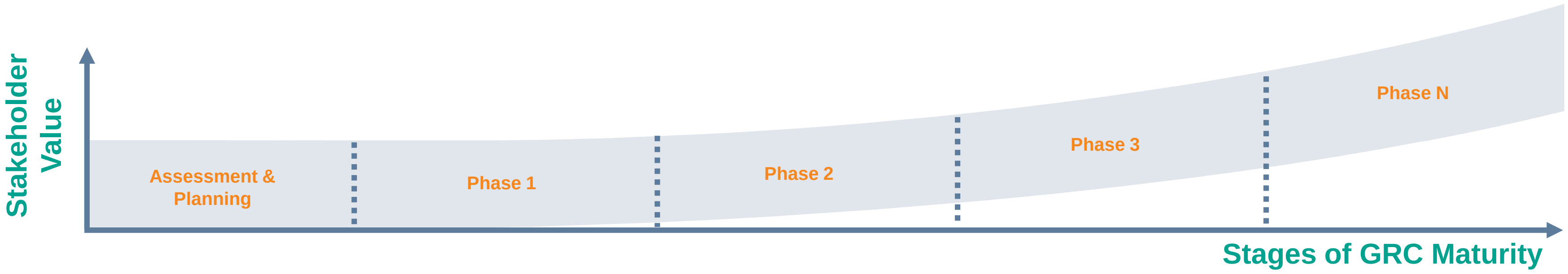
- SAP 's extended support often costs more and thus it might make sense to upgrade to GRC 12.0
- Compliance application enhanced to support business growth and compliance posture



COMMONLY ASKED QUESTIONS

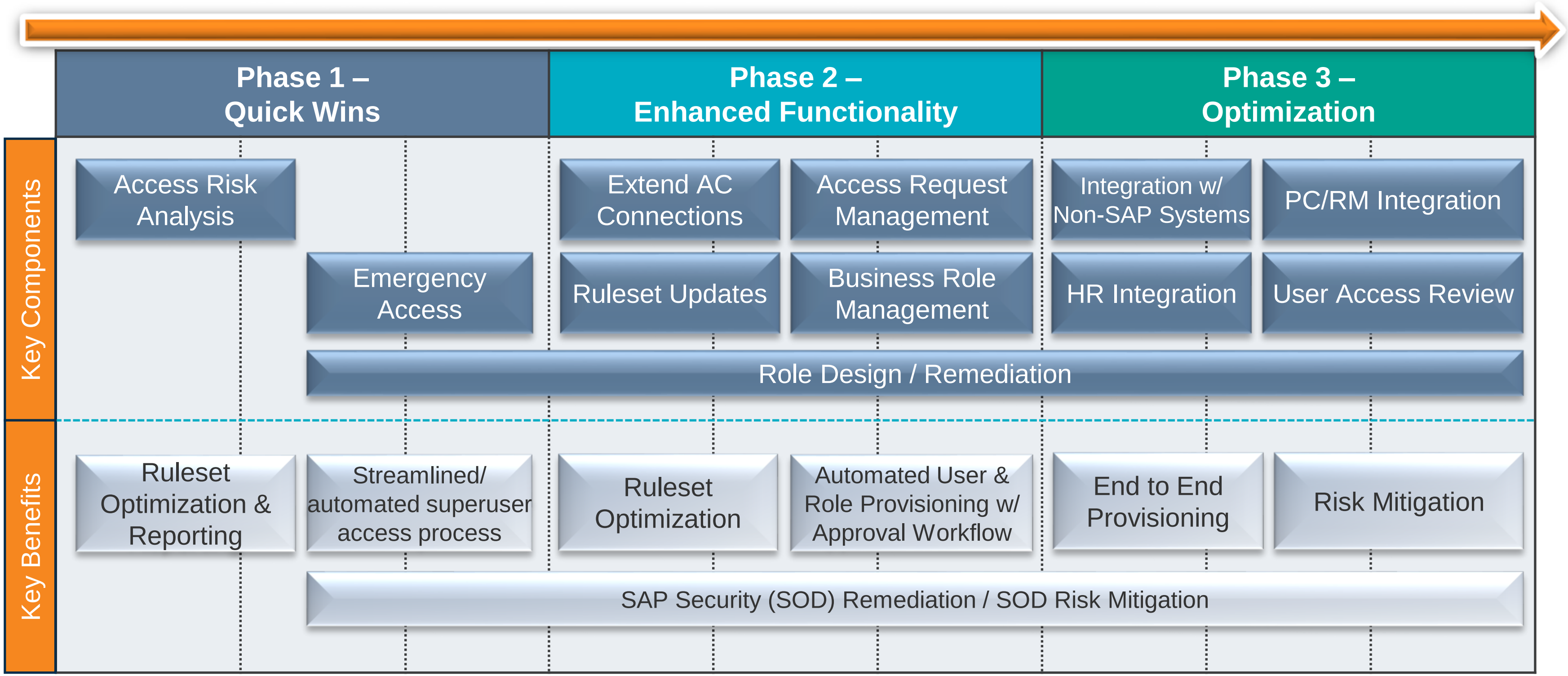
1	**Will GRC 12.0 require Fiori (SAP Gateway Component)?**	No – NWBC (NetWeaver Business Client) will still be supported for users and administrators.
2	**Do we need to be on S/4HANA to take advantage of the unified interface?**	No, however, the Gateway component is required and can be installed with the GRC application.
3	**Will upgrading to GRC 12.0 require HANA?**	HANA is required if you want to take advantage of HANA 3.0 factsheets. For core operational use cases within GRC 12.0, a HANA DB is not required.
4	**Are GRC 12.0 features expected to be made available in 10.1?**	While some of them such as SuccessFactors integration have been down ported to AC 10.1. All new functionality will likely be released as part of GRC 12.0 support pack updates. AC 10.1 support packs will not be released after 12.0 is made generally available.
5	**Will clients need a plugin upgrade in their transactional systems while deploying 12.0?**	No, backward compatibility is provided with version 12.0 as well for plugins on 10.X versions. If organizations want to take advantage of new features, it may require plugin version to be upgraded.

GRC ACCESS CONTROL MATURITY MODEL



Assessment & Roadmap Definition	Monitor and Control SAP Security Risks	Remediate / Optimize SAP Security	Optimize Controls & Enable Continuous Control Monitoring	Enhancements & Proactive Monitoring
• Assess controls and security to determine automation opportunities • Determine technology and process improvement opportunities • Define short and long term roadmap • Establish your Teams	• Enable SOD Risk Analysis & sensitive access reporting (SAP Access Control) • Enable sensitive access monitoring (SAP Access Control) • Customize risk ruleset	• Remediate high priority SOD risks • Redesign security where needed • Automate provisioning • Enable role and user change management • Implement security governance processes	• Review design & documentation of controls – optimize and maximize automated controls • Enable continuous control monitoring – POC of SAP Process Control • Extend scope for SAP continuous control monitoring (CCMs)	• GRC reporting enhancements • Multiple compliance framework and migration of controls to GRC

GRC ACCESS CONTROL – SAMPLE ROADMAP



Phase 1 – Quick Wins

Phase 2 – Enhanced Functionality

Phase 3 – Optimization

Key Components

Access Risk Analysis

Emergency Access

Extend AC Connections

Access Request Management

Ruleset Updates

Business Role Management

Integration w/ Non-SAP Systems

PC/RM Integration

HR Integration

User Access Review

Role Design / Remediation

Key Benefits

Ruleset Optimization & Reporting

Streamlined/ automated superuser access process

Ruleset Optimization

Automated User & Role Provisioning w/ Approval Workflow

End to End Provisioning

Risk Mitigation

SAP Security (SOD) Remediation / SOD Risk Mitigation

CUSTOMER USE CASE

Suketu Patel, Tapestry
November 11th , 2018

PUBLIC

tapestry
COACH | kate spade | STUART WEITZMAN

THE BEST RUN SAP

AGENDA

About Tapestry

Tapestry’s S/4 Journey

- S4 Fashion (1709 release) – Greenfield implementation

Tapestry’s SAP Access Control implementation with S/4

- ARA, ARM and EAM
- CCM

SAP Access Control 12.0 Early Adopter program experience tapestry

COACH | kate spade | STUART WEITZMAN

S4 JOURNEY

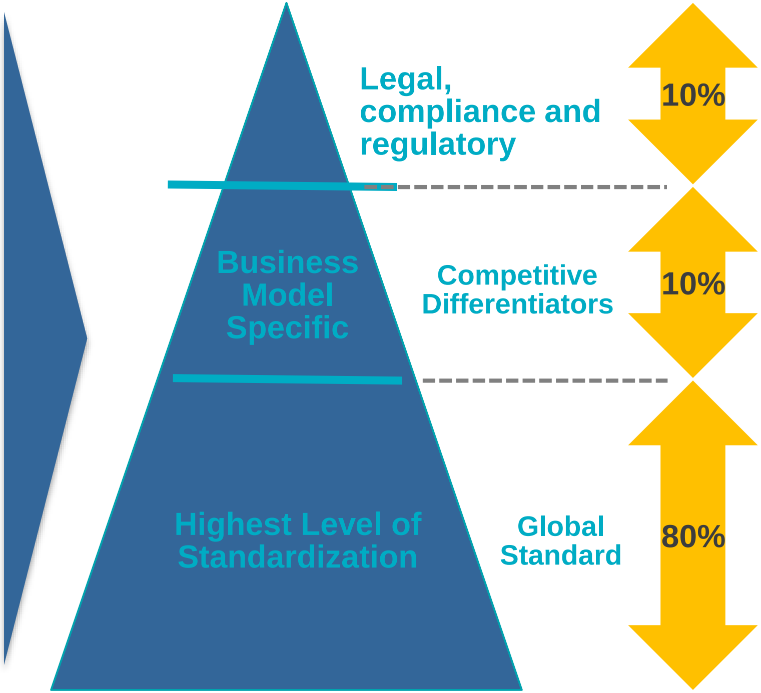
Project Objectives

- *A scalable business model*
- *Speed to M&A readiness*
- *Simplicity and standardization*
- *Improved compliance*
- *Global processes*

Project Scope

- *Global Finance*
- *Sales and WS Order Management*
- *Procurement & Supply Chain*
- *Gross Margin & Inventory Reporting*
- *Master Data Management*

Industry Standards Drive Design


Legal, compliance and regulatory
10%
Business Model Specific
Competitive Differentiators
10%
Highest Level of Standardization
Global Standard
80%

SYSTEMS IN SCOPE WITH GRC

Already Live

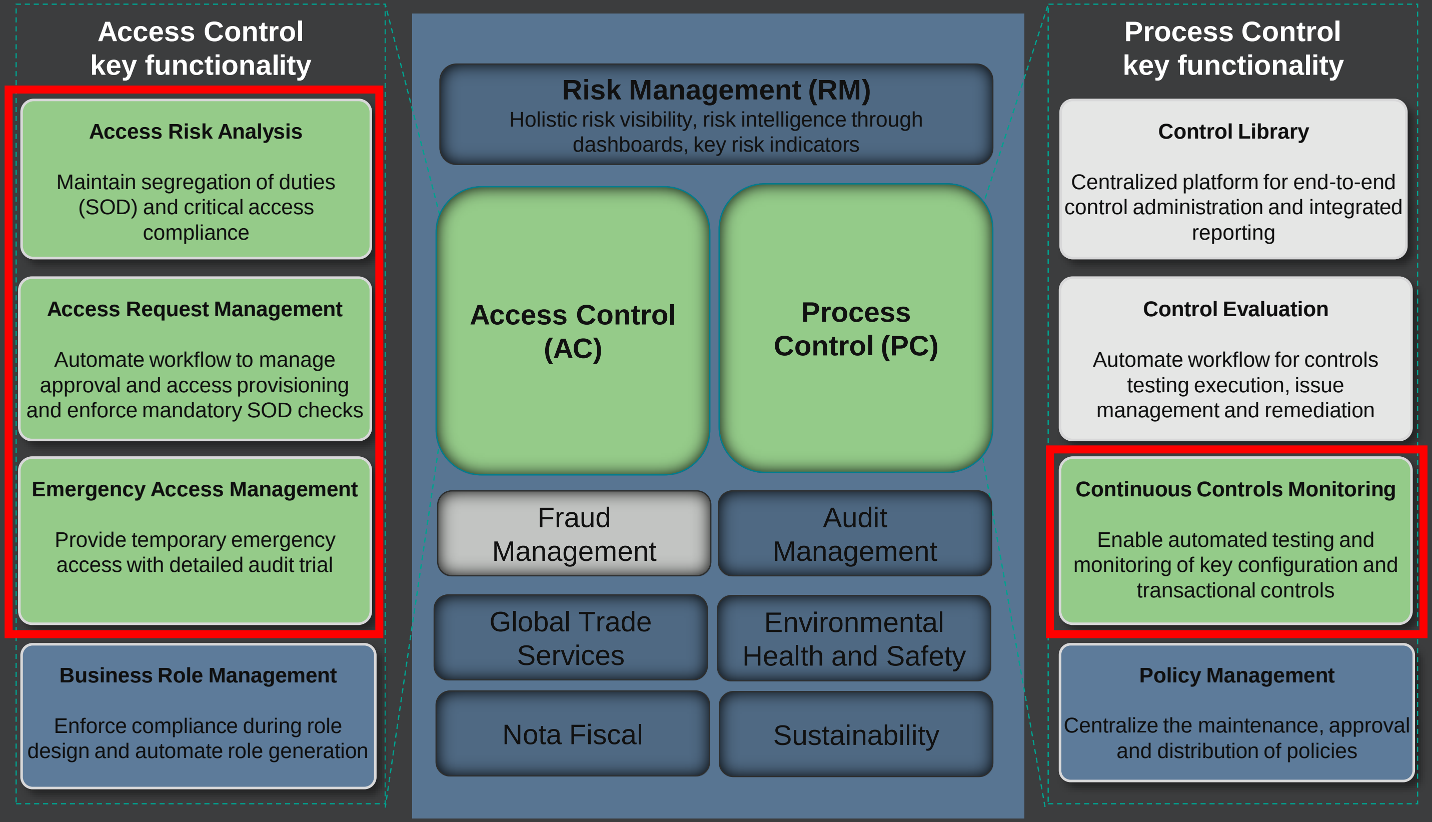
- Employee Central Payroll
- SuccessFactors*
- Business Process and Consolidations
- S/4
- Gateway (Fiori)
- Solution Manager (ChaRM)

- *using Greenlight connector

Future

- Customer Activity Repository (CAR)
- Hana Data Mart
- PI/PO
- Non Production environments

IMPLEMENTATION OF GRC



Access Control key functionality

Access Risk Analysis

Maintain segregation of duties (SOD) and critical access compliance

Access Request Management

Automate workflow to manage approval and access provisioning and enforce mandatory SOD checks

Emergency Access Management

Provide temporary emergency access with detailed audit trial

Business Role Management

Enforce compliance during role design and automate role generation

Risk Management (RM)

Holistic risk visibility, risk intelligence through dashboards, key risk indicators

Access Control (AC)

Process Control (PC)

Fraud Management

Audit Management

Global Trade Services

Environmental Health and Safety

Nota Fiscal

Sustainability

Process Control key functionality

Control Library

Centralized platform for end-to-end control administration and integrated reporting

Control Evaluation

Automate workflow for controls testing execution, issue management and remediation

Continuous Controls Monitoring

Enable automated testing and monitoring of key configuration and transactional controls

Policy Management

Centralize the maintenance, approval and distribution of policies

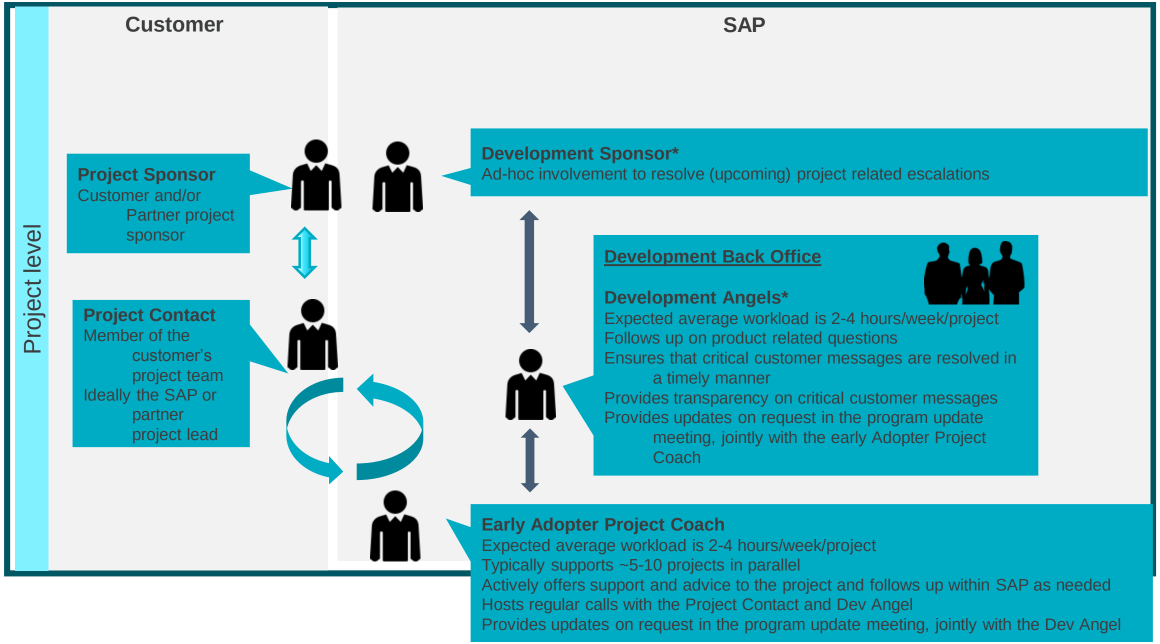
Early Adopter Care Program - Tapestry

SAP Early Adopter Care enabled us to

- Get support with our early implementation of SAP's latest releases via an Early Adopter Care program in close collaboration with SAP with a dedicated back-office support infrastructure in place to safeguard the project and minimize risks
- Access to Stay Current at no additional costs

Impact on SAP

- Direct interaction with development providing first hand feedback
- Bring in the customer voice to influence future releases



Project Sponsor
Customer and/or Partner project sponsor

Project Contact
Member of the customer's project team
Ideally the SAP or partner project lead

Development Sponsor*
Ad-hoc involvement to resolve (upcoming) project related escalations

Development Back Office

Development Angels*
Expected average workload is 2-4 hours/week/project
Follows up on product related questions
Ensures that critical customer messages are resolved in a timely manner
Provides transparency on critical customer messages
Provides updates on request in the program update meeting, jointly with the early Adopter Project Coach

Early Adopter Project Coach
Expected average workload is 2-4 hours/week/project
Typically supports ~5-10 projects in parallel
Actively offers support and advice to the project and follows up within SAP as needed
Hosts regular calls with the Project Contact and Dev Angel
Provides updates on request in the program update meeting, jointly with the Dev Angel

THANK YOU.

- Contact information:

Suketu Patel
Director, Information Security
10 Hudson Yards, New York
212-946-3668

tapestry
COACH | kate spade | STUART WEITZMAN

THE BEST RUN SAP

WRAP UP

Protiviti Perspective provided by David P., Denver

KEY TAKEAWAYS

- S/4HANA landscape introduces 3 security tiers that must be managed.
- Existing ECC security needs to be assessed for new or disabled transactions, and new authorizations in S/4HANA.
- HANA security is different from other tiers in the S/4HANA landscape but many security concepts still apply.
- Security and compliance teams should be integrated early on in the implementation, and key design principles should be established for all tiers.
- Allow adequate time for design and testing, considering the complexity and integration between the 3 layers.
- Advanced SAP security knowledge is essential in developing your new SAP S/4HANA security model.
- Work smart, consider tools to help accelerate your security and GRC efforts.

protiviti®

Face the Future with Confidence

Q&A

KEY SPEAKERS

Peter Creal

SAP

Senior Director,
GRC

peter.creal@sap.com

Phil Jacobs

SAP

Account Executive

p.jacobs@sap.com

Host

Sarma Adithe

SAP

Chief Product Owner,
Access Control

sarma.adithe@sap.com

Kyle Wechsler

Protiviti

Director,
ERP Solutions

kyle.wechsler@protiviti.com

Madhu Mathew

Protiviti

Associate Director,
ERP Solutions

madhu.mathew@protiviti.com

Toni Lastella

Protiviti

Managing Director,
ERP Solutions

toni.lastella@protiviti.com

Host

Suketu Patel

Tapestry, Inc.

Director, IT Risk and
Compliance

spatel2@tapestry.com

protiviti®

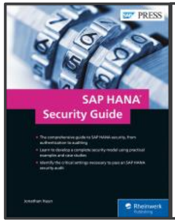
SAP® tapestry

Face the Future with Confidence

protiviti®

REFERENCE MATERIAL

AVAILABLE HANA RESOURCES



SAP HANA Security Guide

SAP Press published Book

2017

Authors: Jonathan Haun

>>View

Implementing SAP HANA

SAP Press published Book

Second Edition 2015

Authors: Jonathan Haun, Chris Hickman, Don Loden, Roy Wells

>>View

SAP HANA High Availability and Disaster Recovery Essentials

SAPinsider & SAP Experts published Journal

2015

>>View

Authors/Contributors: Jonathan Haun

SAP Information Steward: Monitoring Data in Real Time

SAP Press published E-Bite

Aug 2016

Authors: Don Loden

>>View

Creating SAP HANA Information Views

SAP Press published E-Bite

2016

Authors: Jonathan Haun, Chris Hickman, Don Loden, Roy Wells

>>View

Blog Sites:

www.sapbiblog.com (Data & Analytics Blog Site)

https://sapbi.blog (Useful security and SAP HANA Blog)

HANA Webinar Series:

http://bit.ly/HANAwebinars

WHERE TO FIND MORE INFORMATION

GRC on sap.com

- **Governance, risk, and compliance (GRC) solutions:** www.sap.com/grc

General help with SAP governance, risk, and compliance solutions

- **SAP Help Portal:** http://help.sap.com
- **SAP Access Control:** https://help.sap.com/viewer/p/SAP_ACCESS_CONTROL
- **SAP Cloud Identity Access Governance:** https://help.sap.com/viewer/p/SAP_CLOUD_IDENTITY_ACCESS_GOVERNANCE

GRC on analytics from an SAP blog

- **GRC Tuesdays:** http://blogs.sap.com/analytics/category/grc/

Master notes for support packages

Support package	SAP Access Control master note
2369489	Master note for SAP Access Control 10.1 – support pack 16
2407893	Master note for SAP Access Control 10.1 – support pack 17
2448830	Master note for SAP Access Control 10.1 – support pack 18
2494105	Master note for SAP Access Control 10.1 – support pack 19

WHERE TO FIND MORE INFORMATION

Take a look at:

www.sap.com/GRC

www.sap.com/security

www.sap.com/finance

Follow our blogs:

GRC Tuesdays

Find detailed information:

https://www.sap.com/products/cloud-iam.html

Follow us on Twitter:

#SAPGRC

Home › Products › Finance

Governance, Risk, and Compliance

WHERE TO FIND MORE INFORMATION

- https://help.sap.com/doc/4698ca4ad85a4a24994b2016f366cc77/1709%20000/en-US/SIMPL_OP1709.pdf
  - “SAP Simplification List for SAP S/4HANA 1709 Initial Shipment Stack” (SAP, December 2017).
- www.protiviti.com/US-en/insights/securing-your-sap-hana-environment
  - Protiviti, “SAP HANA Implementation Webcast” (May 2016).
- www.protiviti.com/US-en/insights/dont-leave-grc-behind
  - “Moving to SAP® S/4HANA? Don’t Leave GRC Behind” (Protiviti).
- https://help.sap.com/viewer/742945a940f240f4a2a0e39f93d3e2d4/2.0.02/en-US/a840530a2ab64d2188aa95d503a003a3.html
  - “Checklist for Secure Handover” (SAP).
- https://help.sap.com/viewer/742945a940f240f4a2a0e39f93d3e2d4/2.0.02/en-US/45955420940c4e80a1379bc7270cead6.html
  - “Recommendations for Database Users, Roles, and Privileges” (SAP).

WHERE TO FIND MORE INFORMATION

- www.protiviti.com/US-en/insights/wp-sap-access-management-governance-sustainability
  - “SAP Access Management Governance: Getting It Right, Making It Sustainable” (Protiviti).
- www.protiviti.com/US-en/insights/managing-sap-access-control-10
  - “Managing the SAP Access Control” (Protiviti).
- www.protiviti.com/US-en/insights/wp-continuous-monitoring-and-control-automation-sap
  - “Unlocking the Value of Continuous Monitoring and Control Automation Capabilities in SAP Process Control” (Protiviti).
- https://help.sap.com/viewer/742945a940f240f4a2a0e39f93d3e2d4/2.0.02/en-US/5c34ecd355e44aa9af3b3e6de4bbf5c1.html
  - “Recommendations for Audit” (SAP).