

EPI·USE[®]



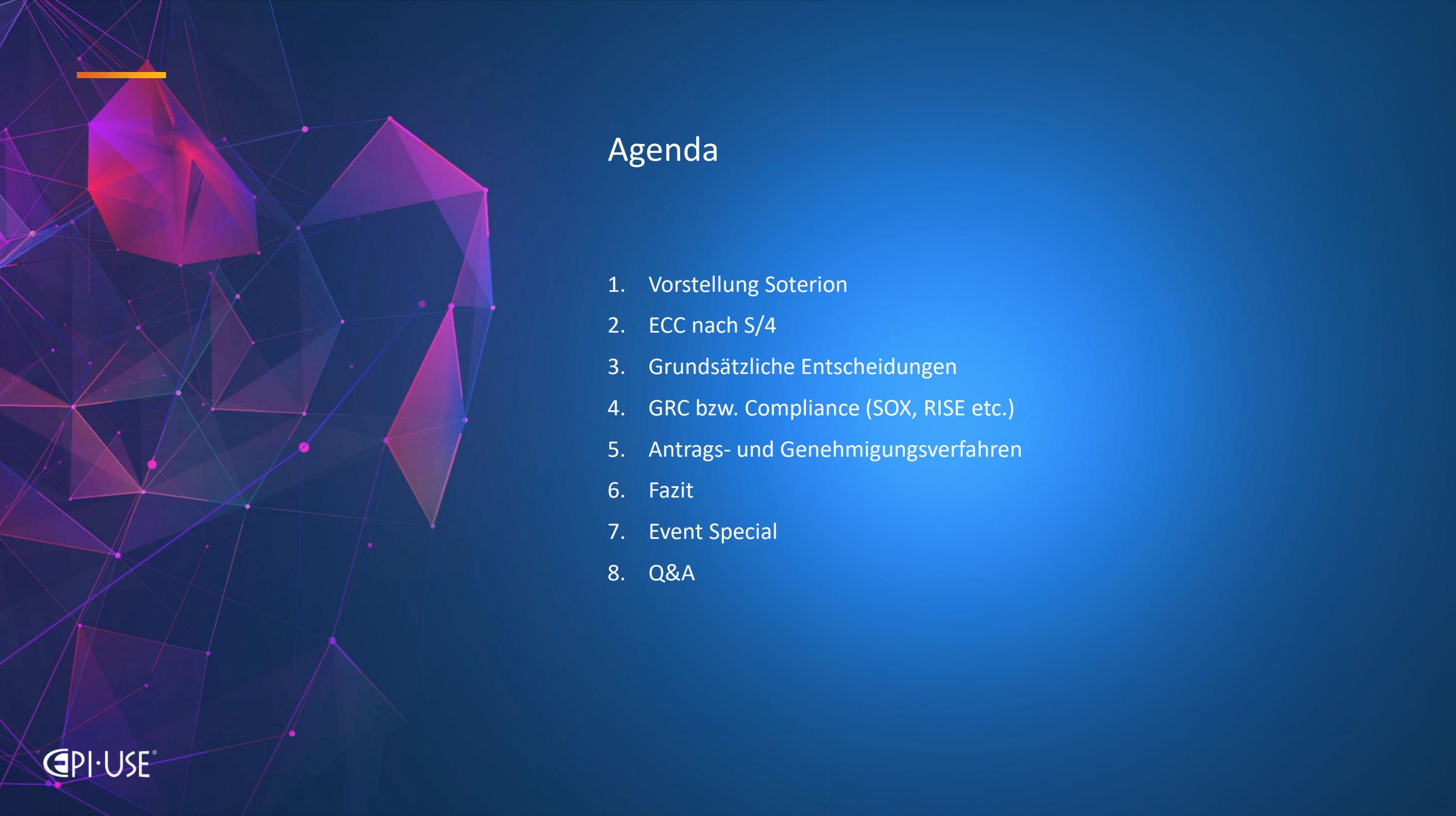
 **soterion**

Effektive, automatisierte GRC-Analyse für SAP S/4HANA

11 Tipps für Ihre S/4HANA Sicherheit

Andreas Knab, VP Sales D-A-CH

18.09.2024



Agenda

1. Vorstellung Soterion
2. ECC nach S/4
3. Grundsätzliche Entscheidungen
4. GRC bzw. Compliance (SOX, RISE etc.)
5. Antrags- und Genehmigungsverfahren
6. Fazit
7. Event Special
8. Q&A



soterion

Rollen, User,
Compliance,
Risiken,
Lizenzen etc.
(GRC)

160 Kunden

11 Jahren am
Markt

Soterion Technologies
GmbH
Stuttgart Airportcenter

100 bis 100.000
User

Access Risk Manager

Basis Review Manager

Central Identity Manager

Data Privacy Manager

Elevated Rights Manager

Materialised Risk Manager

Password Self-Service

Periodic Review Manager

SAP License Manager

SuccessFactors

**Product
Demo**

Access Risk Manager (Identify Risk)



„Erinnern“ wir uns zuerst an das ECC...

Zu wenig
interne
Ressourcen für
Berechtigungen

„Gib dem Mayer
mal die
Berechtigungen
...ähhh... die der
Müller hat“

„Hey Paul, gib
mir mal die
SE16“

„Monster-
Rollen“ mit
Findings im
Audit

Intransparente
oder
komplizierte
Anträge ohne
Änderungs-
historie

Frustration für
Antragsteller
und Freigeber

Wunsch

Sicheres und effizientes S/4 System
mit Einhaltung der Compliance

Wie geht es jetzt weiter im S/4?

„Gib dem Mayer mal die Berechtigungen ...ähhh... “ ist ok wenn ich verstehe, was ich verursache

Weitreichende Berechtigungen sind bei der S/4 Einführung oft die Regel

Fehlende Berechtigungen sollen die Einführung nicht behindern

TIPP Nr.1:
Frühzeitige GRC-Toolauswahl. Prozesse und Features definieren und zuerst die größten Risiken erkennen/entfernen

Go-Live mit offenem Scheunentor sollte vermieden werden

Fiori Services führen im S/4 Betrieb zu noch mehr Konfusion und Wildwuchs als im ECC

Antrags- und Genehmigungsprozesse müssen leicht verständlich sein

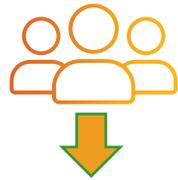
Weitreichende Berechtigungen könnten über einen Firefighter Prozess kontrolliert werden

Temporäre Entscheidungen können z.B. nach wenigen Monaten rezertifiziert werden



Grundlegende Entscheidungen

Entscheidung: Wie viel Schutz benötige ich für mein S/4?



Business-centric GRC

TIPP Nr.2:
Beachten Sie das bekannte Prinzip der Wirtschaftsprüfer „Three Lines of Defense“

**ERSTE
LINIE**
Business User
(Viele Personen)

 soterion

**ZWEITE
LINIE**
Profis
(Einzelne Personen)

 soterion

**DRITTE
LINIE**
Auditoren
(Post mortem Sicht)

 soterion

Entscheidung: Angemessener Aufwand in Relation zum Nutzen

Time to Value

Sofort die Compliance-Risiken verstehen

**TIPP Nr.3:
Fokussieren Sie sich zunächst auf das Wesentliche**

Tagesgeschäft:
 • Anträge
 • Genehmigungen
 • Analysen
 • Bereinigungen
 • KVP

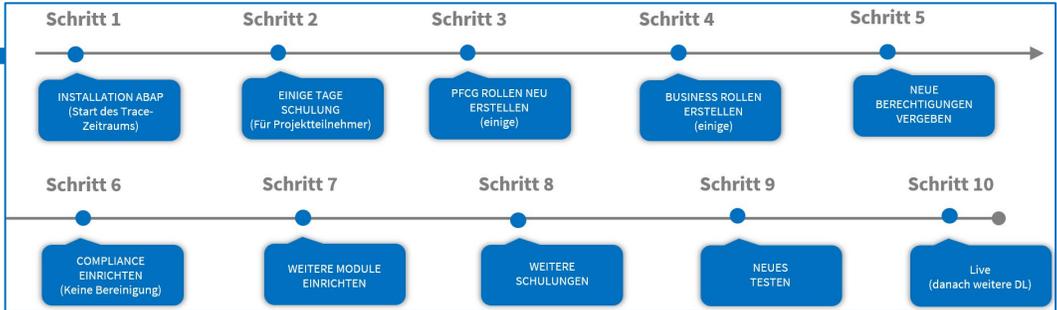
Live:
 Soterion: ca. 5 PT zzgl.
 Kunde: ca. 3-5 PT

soterion

„LIVE“ SCHON IM POC

Bestehendes Cloud-System auf MS-AZURE wird genutzt
 Schulung findet im POC statt
 Bestehende Rollen werden bestmöglich genutzt
 Business-Rollen werden schon im POC erstellt
 Rollen-Zuordnungen können zuerst weiter verwendet werden
 Compliance entsteht von der ersten Minute an

Tagesgeschäft:
 • Anträge
 • Genehmigungen
 • Analysen
 • Bereinigungen



Live:
 Anbieter: ca. 30-100 PT zzgl.
 Kunde: ca. 60-200 PT

Realität

Teilprojekt z.B.:

- Anpassung der SOD (z.B. Z-Transaktionen)
- Anpassung der Business-Rollen
- Anpassung der SAP Lizenzen
- Anpassung der kompensierenden Kontrollen
- Bereinigung der Konflikte
- Anpassung der pfcg Rollen

Durchschnittlicher Aufwand PT bis zum Live-Betrieb. Andere Anbieter vs. Soterion



S/4HANA Compliance

S/4 Rollen entschärfen oder neu generieren?

Welche Rollen bereiten Probleme?

Compliance

Zuerst neues S/4 Rollenset?

Neues Rollenset

Ziel im S/4:

- **Sicheres System**
- **Einhaltung der Vorgaben**
- **Angemessener Aufwand in Relation zum Nutzen**

TIPP Nr.4:

Nutzen Sie Analyse-Tools für Ihre Rollen, um ein komplettes Re-Design möglichst zu vermeiden.

Beispiel Rollen Assistenten

The screenshot displays the 'Bewältigen' (Manage) interface in the Soterion system. The top navigation bar includes a logo, the title 'Bewältigen', and several dropdown menus: 'Überfl. Rollen', 'Überfl. Transaktionen', 'Bereinigungsassistenten', and 'Sehen, was möglich ist'. The 'Bereinigungsassistenten' menu is highlighted with a red circle and is open, showing a list of cleaning assistant options. The main content area features a 'Risiken' (Risks) section with a comparison of 'Potentielle Risiken' (4,967) and 'Tatsächliche Risiken' (1,352), along with a 'Bereinigungspotential' (Cleaning Potential) of 15%. On the right, there are two large blue panels with user icons and counts: 31,372 and 663. A vertical sidebar on the left contains various system icons.

Bewältigen Überfl. Rollen ▼ Überfl. Transaktionen ▼ **Bereinigungsassistenten ▼** Sehen, was möglich ist ▼

Risiken

Potentielle Risiken	Tatsächliche Risiken
4,967	1,352

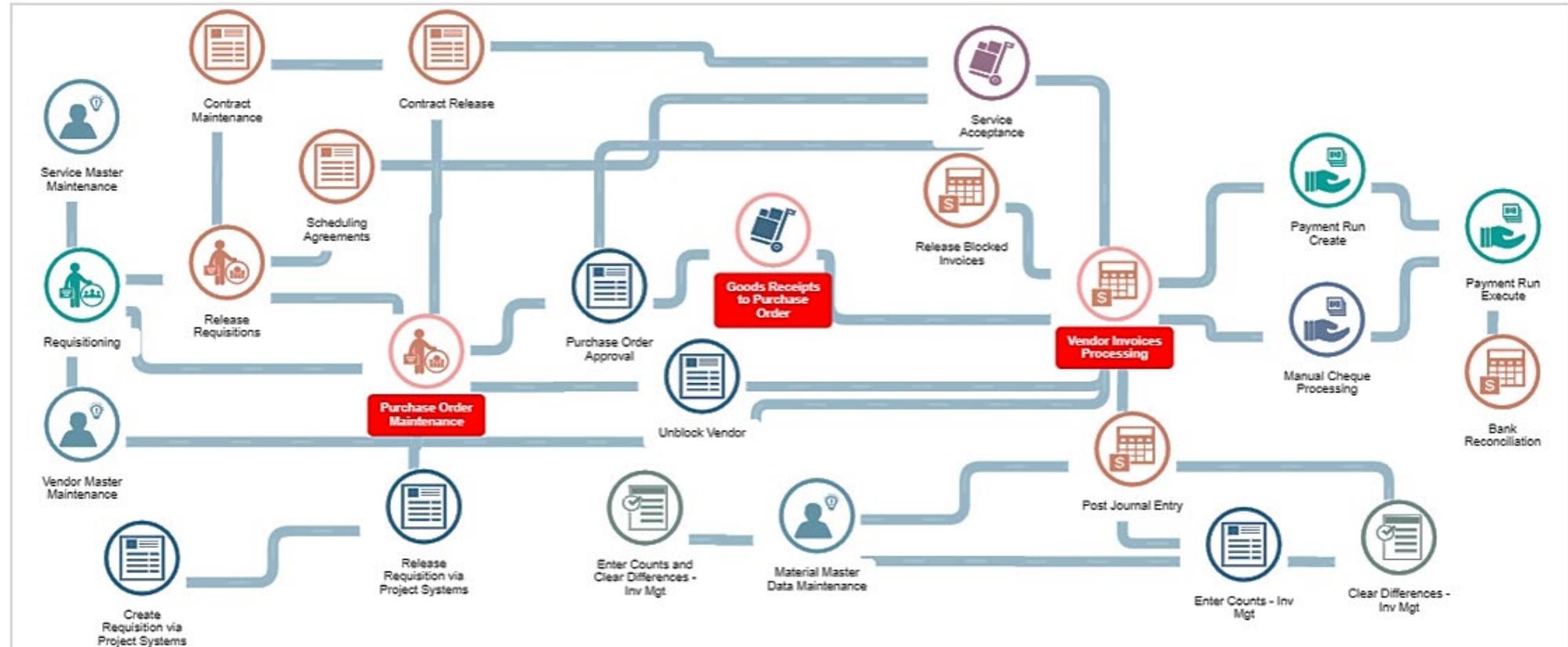
Bereinigungspotential
15 %

31,372

663

- Rollenspaltung
- Bereinigung Sammelrolle
- Überfl. Rollenbereinigung
- Rolle Löschen
- Transaktion Löschen
- Rollenstandardisierung
- Rolle für Gruppe von Benutzern
- Worklist-Items

S/4 Prozesse leicht verständlich



TIPP Nr.5:

Lassen Sie sich die Risiken visualisieren. So schaffen Sie die notwendige Risiko-Sensibilität im S/4.

Rezertifizierung User Access (SOX)

TIPP Nr.6:
Rezertifizierung kann schnell und effizient über Geschäftsprozesse abgebildet werden.

Überprüfung Inbox

Nach Geschäftsprozess filtern

H2R 23 BA 6 FI 12 MM 3 P2P 12 O2C 8 PP 1

Zu überprüfende Elemente Funktionalen Zugriff genehmigen Risiken ansehen

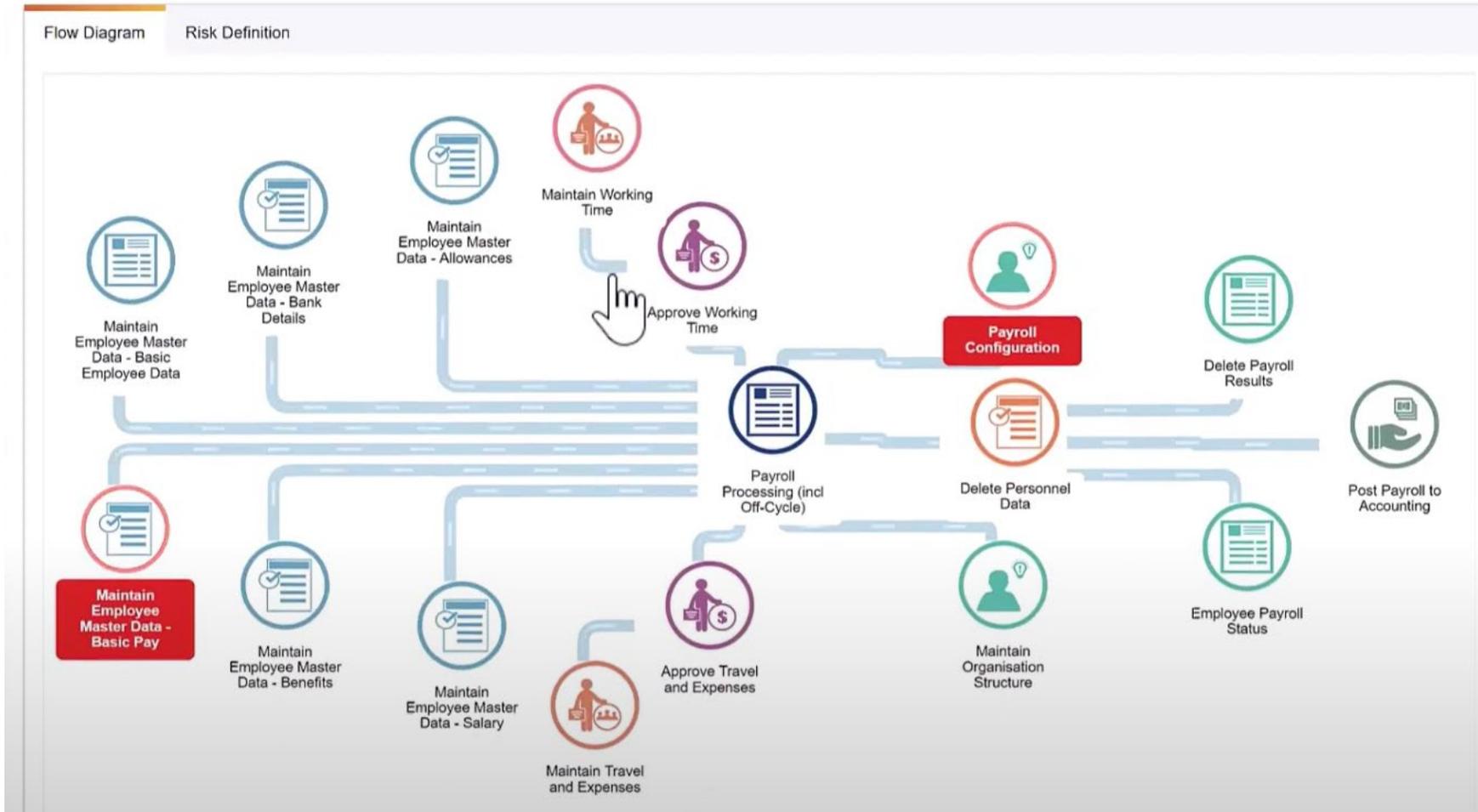
Die Transaktionsverwendung basiert auf dem Datum des letzten Imports und nicht auf dem Erstellungsdatum für das Überprüfungsset.

Drag a column header here to group by that column

#	Sperr...	Benutzername	Benutzer...	Rolle	SAP-System	Über Gesch...	Trans. in Rolle	Trans.-verwen...	T... z... R... bei	Zuvor überprüft
		RPEARSON (Rocco Pearson)	AA00	ZF_MP_PUR_ORD_PROCESSING_SENS (MP - Purchase Order Processing Sensitive)	ECC (OEP)		4	0	✓	👍
		JRAMPLING1 (Jake Rampling)	AA00	ZF_MP_PUR_ORD_PROCESSING_SENS (MP - Purchase Order Processing Sensitive)	ECC (OEP)		4	43	✓	👍

Out of the box Regelwerk auch für SuccessFactors

H2R04.01 (User is able to complete payroll configuration & maintain employee - Basic pay) **Medium**



Simulationen verhindern Wildwuchs und überflüssige Workflows

TIPP Nr.7:
Simulieren Sie
Änderungen in Ihrer
Berechtigungslandschaft
bevor Sie diese auf SAP
übertragen

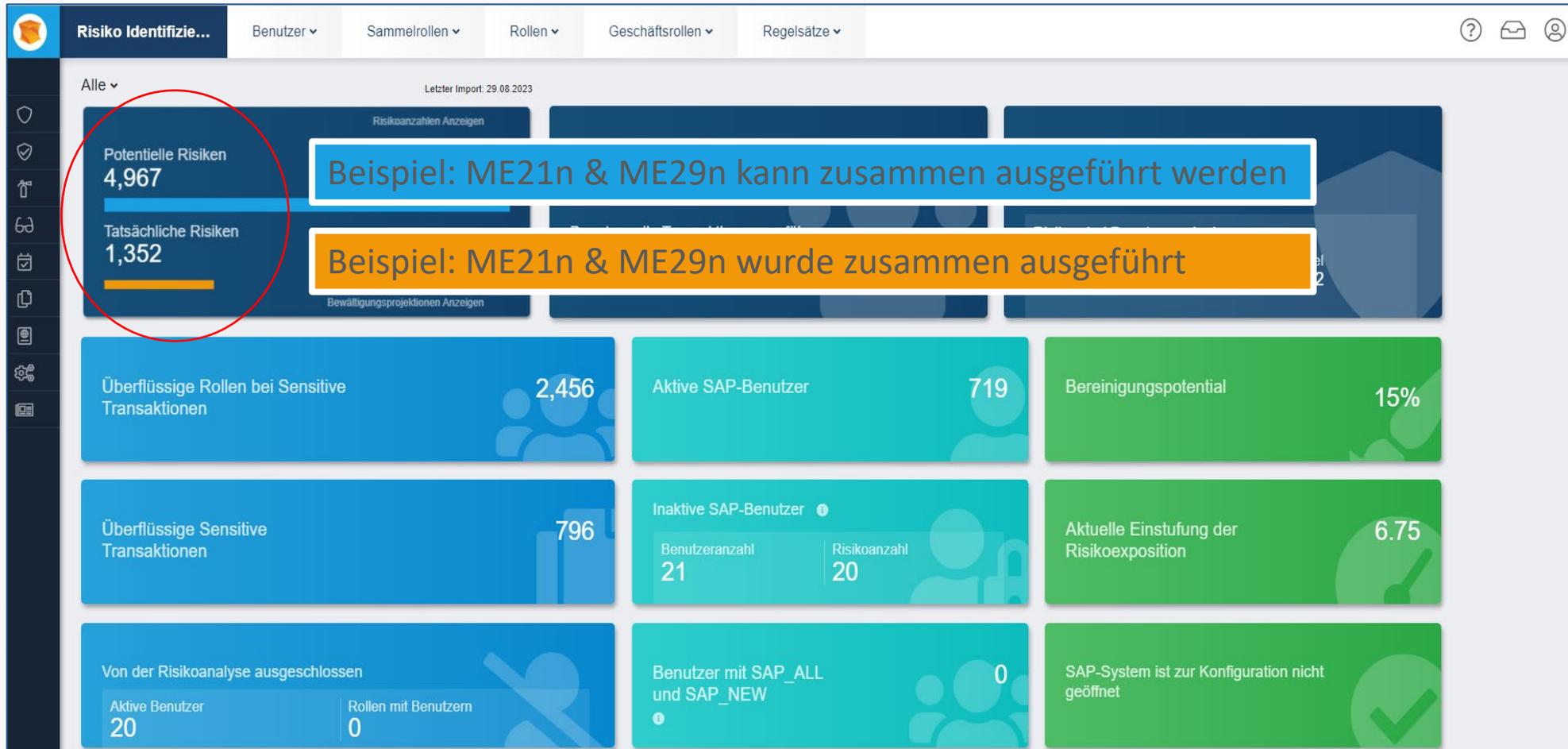
The screenshot shows a web interface with a navigation bar at the top containing three tabs: '1 Typ', '2 Simulation-Auswahl', and '3 Ergebnisse'. The '2 Simulation-Auswahl' tab is active and circled in red. Below the navigation bar, the main content area is titled 'Zugriffsrisiko Simulationen' and includes the instruction: 'Simulieren Sie Änderungen in Ihrer Berechtigungslandschaft, bevor Sie diese auf SAP übertragen.' The interface is divided into four main simulation categories, each with a list of actions:

- Rollensimulationen** (Simulieren Sie die Auswirkungen der Zuordnung oder Entfernung von Elementen aus einer Rolle):
 - Benutzer der Rolle zuordnen (with arrow icon)
 - Rollen der Sammelrolle zuordnen (with arrow icon)
 - Rollen aus der Sammelrolle löschen (with arrow icon)
 - Neue Rolle anlegen
 - Rolle für Transport analysieren (with star icon)
- Benutzersimulationen** (Simulieren Sie die Auswirkungen der Zuordnung oder Entfernung von Elementen):
 - Rollen dem Benutzer zuordnen (with arrow icon)
 - Stellen dem Benutzer zuordnen
 - Neuen Benutzer anlegen (with arrow icon)
 - Rollen aus Benutzer Löschen (with arrow icon)
 - Benutzersersetzung (with arrow icon)
 - Benutzer freischalten und erweitern (with arrow icon)
- Stellensimulationen** (Simulieren Sie die Auswirkungen der Zuordnung oder Entfernung von Elementen aus einer Stelle):
 - (No actions listed)
- Geschäftsrolle Simulationen** (Simulieren Sie die Auswirkungen der Zuweisung von Rollen und Benutzern zu einer Geschäftsrolle):
 - (No actions listed)

At the bottom right, there are two legend items:

- ★ Simulation ist nicht workflowfähig
- ↗ An SAP Bereitstellen ⓘ

Risiko bzw. SoD Analysen von potenziellen und tatsächlichen Risiken



Risiko Analysen Details

Risiko Identifizie... Benutzer ▾ Sammelrollen ▾ Rollen ▾ Geschäftsrollen ▾ Regelsätze ▾

Risikostatistik des Benutzers Risiken pro Benutzer Benutzeranzahl Pro Risiko

Alle Risikotypen ▾ Critical ▾

Alle Risikotypen
Kritische Transaktionen
SoD
Datenschutz

Name	Abteilung	Benutzergruppe	Sperrz...	Abgelaufen	Benutz...	Lizenz Typ	Von der Analyse ausgeschl...	Bewegung	Poten... Risiken	Tatsächliche Risiken
RMAY1 Rachel May	Amawandle Pelagic - Finance	DD00			A (Dialog)	SAP Applicati...			3	27
JDAVIES4 Jane Davies	LSO Hout Bay - Finance	CD00			A (Dialog)	SAP Applicati...			3	27

Risikostatistik des Benutzers Risiken pro Benutzer Benutzeranzahl Pro Risiko

Benutzer ▾

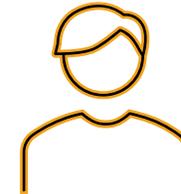
Vollständiger Name	Sperr...	Abgel...	Typ	Abteilung	Risiko	Risikotyp	Risikostufe	Potentielle Risiken	Ist tatsächl... Risiko
Benutzer: AALLAN									
Alexander Allan			A (Dialog)	BCP - Hake Finance	CT_MM03 (Critical Transactions MATERIALS MANAGEMENT: Maintain Material Cost - Price Cha...	CriticalTrans	High	1	✓
Alexander Allan			A (Dialog)	BCP - Hake Finance	CT_SD04 (Critical Transactions SALES & DISTRIBUTION: Confirm Customer Master Changes)	CriticalTrans	High	2	✓
Alexander Allan			A (Dialog)	BCP - Hake Finance	MAT05 (User is able to receive/issue incorrect amount of inventory & clear differences via IM)	SOD	High	2	✓
Alexander Allan			A (Dialog)	BCP - Hake Finance	PUR22 (User is able to approve the purchase of unauthorized item & hide it by not fully receiving ...)	SOD	High	2	✓
Alexander Allan			A (Dialog)	BCP - Hake Finance	PUR25 (User is able to release an order & initiate payment)	SOD	High	2	✓
Alexander Allan			A (Dialog)	BCP - Hake Finance	PUR51 (User is able to hide inventory by not fully receiving the order & initiate payment by invoic...	SOD	Critical	1	✓
Alexander Allan			A (Dialog)	BCP - Hake Finance	PUR60 (User is able to release blocked invoices & initiate payments by invoicing)	SOD	Critical	2	✓
Benutzer: ABERNARD									
Benutzer: ABUCKLAND									

Mehr als nur SoD Analyse

SoD-Verstöße im Betrieb automatisch überwachen

Betrieb mit automatisierter SoD-Compliance (Prozesskontrolle)

The screenshot displays a web application interface for risk management. At the top, there's a navigation bar with 'Materialised Risk' and various menu items. The main content area shows 'Case Details: Case 63' with tabs for 'Summary', 'Events', 'Purchase Order', 'Investigation', and 'Audit Log'. The 'Summary' tab is active, showing a form with fields for 'SAP System', 'Risk', 'Risk Level', 'Risk Owner', 'Risk Owner Group', and 'Executed By'. A red oval highlights the 'Status' section, which includes 'Assigned To Risk Owner Group' (MAT Risk Owner), 'Status' (Under Investigation), and a 'Save' button. Below the main interface, two panels show function configuration details. The left panel is for 'Function Name: MP_POM' with 'Description: Purchase Order Maintenance'. The right panel is for 'Function Name: MP_POA' with 'Description: Purchase Order Approval'. Both panels have a 'Purchase Order' section with fields for 'PO Number', 'PO Created On', 'Document Type', 'Last Released On', 'PO Value', 'Last Released By', and 'PO Value (Base Currency)'. Red ovals highlight the 'Description' and 'PO Number' fields in both panels.

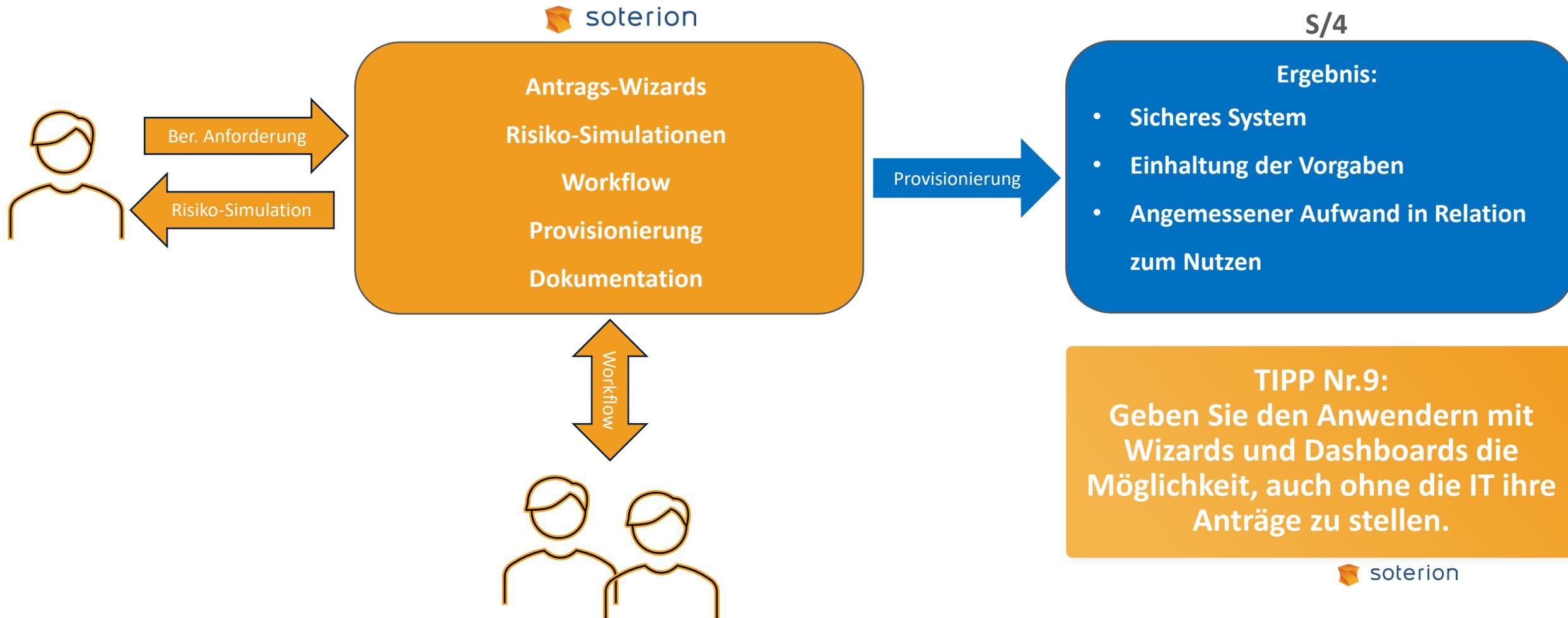


TIPP Nr.8:
Nutzen Sie automatisierte Systeme für die Kontrolle geschäftskritischer Prozesse.

Was ist wichtig für den Fachbereich?

Sichere und verständliche Antrags- und Genehmigungsverfahren

Antrags- und Genehmigungsverfahren für Fachbereiche



Beispiel: Wizard in drei Schritten

1 Typ 2 Simulation-Auswahl 3 Ergebnisse

Zugriffsrisiko Simulationen

Simulieren Sie Änderungen in Ihrer Berechtigungslandschaft, bevor Sie diese auf SAP übertragen.

Rollensimulationen
Simulieren Sie die Auswirkungen der Zuordnung oder Entfernung von Elementen aus einer Rolle

Benutzersimulationen
Simulieren Sie die Auswirkungen der Zuordnung oder Entfernung von Elementen

Rollen dem Benutzer zuordnen

1 Typ 2 Simulation-Auswahl 3 Ergebnisse

Rollen dem Benutzer zuordnen

Benutzer auswählen: AALLAN (Alexander Allan) x

Rollen zuordnen: ZF_MP_PUR_ORD_PROCESSING_SENS x

Gültig ab: 26.04.2024

Gültig bis: 31.12.9999

Werte Löschen Rollen von einem anderen Benutzer kopieren Simulation ausführen

Benutzer auswählen: einer Stelle

Rollen zuordnen: Geschäftsrolle

Berechtigungsrollen

Berechtigungsrollen
Simulieren Sie die Auswirkungen der Zuordnung von Berechtigungsobjekten

★ Simulation ist nicht workflowfähig

➤ An SAP Bereitstellen

Beispiel: Wizard Ergebnis

The screenshot displays a three-step wizard process. Step 3, 'Ergebnisse', is highlighted with a red circle. The 'Zusammenfassung' section features a red warning banner: 'Führt Zu Neuem Risiko'. Below this, three panels provide details: 'Benutzer' (AALLAN (Alexander Allan)), 'Rollen' (ZF_MP_PUR_ORD_PROCESSING_SENS (MP - Purchase Order Processing Sensitive) with counts 1, 2, 1), and 'Risikoänderung' (2 Kritisch, 1 Hoch). Two buttons are present: 'Workflow-Element anlegen' and 'Genehmigungs-PDF erstellen'. The 'Detail' section, titled 'Dieser Antrag verursacht neue Risiken', lists three risks with severity levels: PUR28 (Kritisch), PUR29 (Hoch), and PUR61 (Kritisch). An orange arrow points to the information icon of the first risk. A filter button 'Nach Geschäftsprozess filtern' and a link 'Alle Risiken aufklappen' are also visible.

1 Typ 2 Simulation-Auswahl 3 Ergebnisse

Zusammenfassung

⚠ Führt Zu Neuem Risiko

Benutzer AALLAN (Alexander Allan)	Rollen ZF_MP_PUR_ORD_PROCESSING_SENS (MP - Purchase Order Processing Sensitive) 1 2 1	Risikoänderung 2 Kritisch 1 Hoch
---	---	--

Workflow-Element anlegen Genehmigungs-PDF erstellen

Detail

Dieser Antrag verursacht neue Risiken Nach Geschäftsprozess filtern

AALLAN (Alexander Allan) Alle Risiken aufklappen

✓ PUR28 (User is able to purchase unauthorized items & initiate payment by invoicing)	i	Kritisch
✓ PUR29 (User is able to purchase unauthorized items & hide it by not fully receiving order)	i	Hoch
✓ PUR61 (User is able to maintain & approve Purchase Orders)	i	Kritisch

„Papierantrag“ via PDF oder Workflowantrag

Beispiel: Wizard Ergebnis mit Fiori Findings

✓ MAT05 (User is able to receive/issue incorrect amount of inventory & clear differences (IM))	
^ PUR22 (User is able to approve the purchase of unauthorized items & hide inventory by not fully receiving the order)	
Role	Transaction
Function: MM_GRP (Goods Receipts to Purchase Order)	
ZF_MM_MATERIAL_GOODS_MOVE_DIS (MM - Material Goods Movement Display)	MIGO (Goods Movement)
Function: MP_POA (Purchase Order Approval)	
ZF_MP_PUR_ORD_RELEASE (MP - Purchase Order Release)	GBAPP_POAPPROVAL (Fiori Service)
ZF_MP_PUR_ORD_RELEASE (MP - Purchase Order Release)	ME28 (Release Purchase Order)
ZF_MP_PUR_ORD_RELEASE (MP - Purchase Order Release)	ME29N (Release purchase order)
ZO_MM_RELEASE_GRP_B1_CDE_ET (MM - Value Role for Purchasing Release Strategy - Group B1 & Code ET)	GBAPP_POAPPROVAL (Fiori Service)
ZO_MM_RELEASE_GRP_B2_CDE_ET (MM - Value Role for Purchasing Release Strategy - Group B2 & Code ET)	GBAPP_POAPPROVAL (Fiori Service)
ZO_MP_PURCH_DOC_NB_ALL (MP - Purchase Document type NB Purchase Requisition and PO All)	GBAPP_POAPPROVAL (Fiori Service)

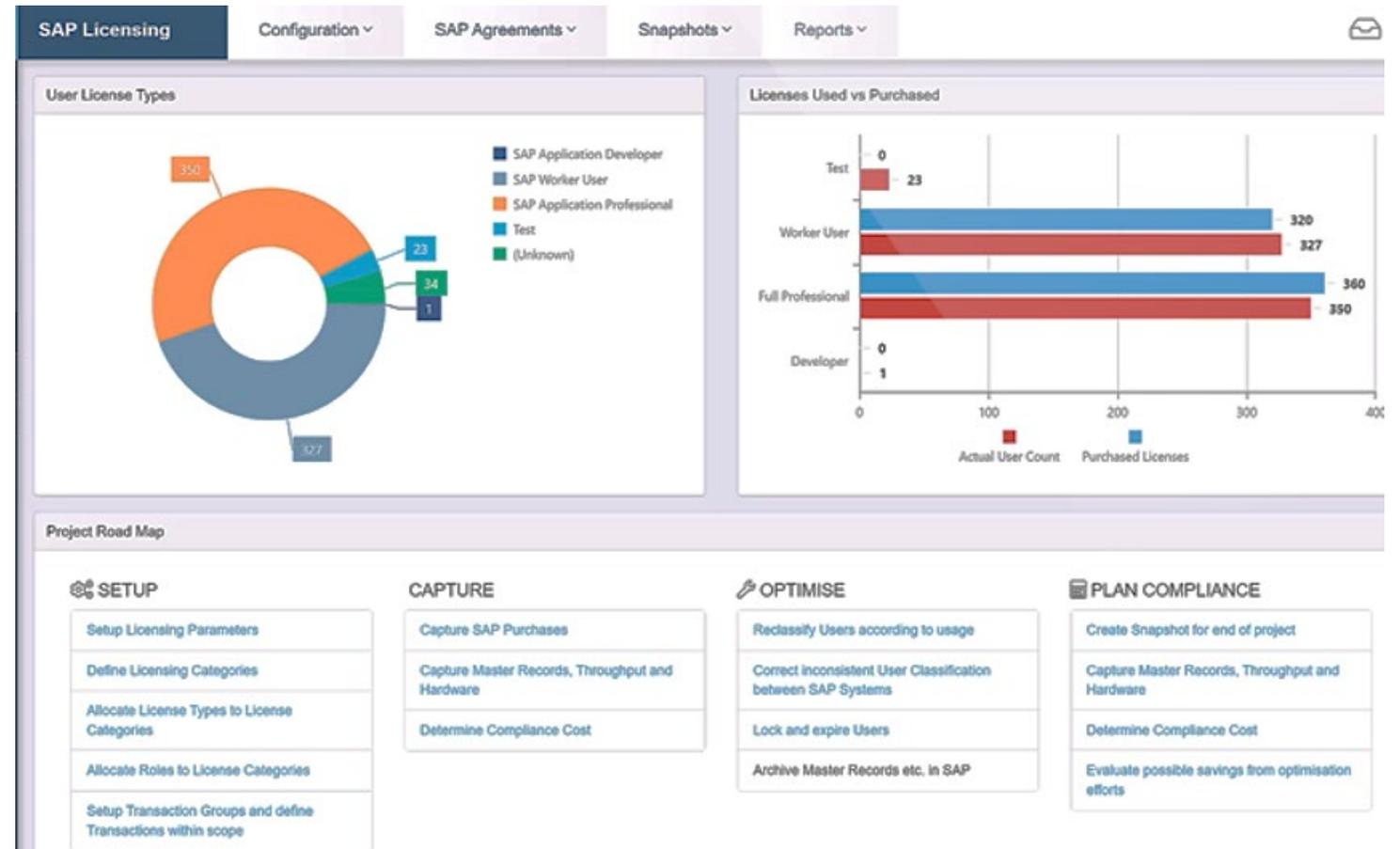
S/4HANA Cloud bzw. RISE:

Wichtiger Hinweis:

Bei der Migration auf S/4HANA Cloud oder SAP RISE kann sich das Lizenzierungsmodell ändern. Künftig erfolgt die Abrechnung häufig auf Basis der zugewiesenen Berechtigungen. Schlanke Berechtigungen können Lizenzkosten einsparen.

TIPP Nr.10:
Versuchen Sie ungeachtet der „Faktenlage“, Ihre Preise mit SAP zu verhandeln

Eine Bitte in eigener Sache zum Thema SAP Star Analyse:
Unterstützen Sie uns bei der künftigen Lizenzierungs-
Analyse.



Fazit:

**GRC bzw. Access & Authorization im
SAP S/4HANA muss mit hoher Priorität
und Sorgfalt behandelt werden.**

**Auch ohne große Projekte lassen sich
mit effizienten Tools in kürzester Zeit
zuverlässige und sichere Lösungen für
SAP S/4HANA entwickeln.**

**TIPP Nr. 11:
Die richtige Lösung, in Kombination mit bestehender Infrastruktur, stellt die
benötigten Funktionen sofort bereit und unterstützt so effizient die Umsetzung
des Three Lines of Defence-Modells.**



Wo stehe ich mit meiner Compliance?

Inspire 2024 Angebot:

Risiko Quick-Check mit konkreten Handlungsempfehlungen



Die Benutzer, bei denen es zu Funktionstrennungskonflikten (SoD) und kritischen Transaktionszugriffen kommt



Die Rolle/das Profil, von dem der Benutzer diesen Zugriff erhält



Ob der Benutzer die Transaktionscodes ausführt



Vorschläge zur Rollenbereinigung oder Risikobehhebung, die durchgeführt werden könnten, um das Zugriffsrisiko der Organisation zu verringern.



Questions





Vielen Dank!



EPI-USE Labs GmbH | Altrottstr. 31 | 69190 Walldorf
Sitz der Gesellschaft: Walldorf, Deutschland | Geschäftsführer: Henrik Stammer, Lars Fuchs
Amtsgericht Mannheim HRB710994

