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

„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

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 Genehmigungs-prozesse müssen leicht verständlich sein

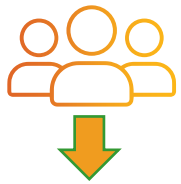
Weitreichende Berechtigungen könnten über einen Firefighter Prozess kontrolliert werden

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

Grundlegende Entscheidungen

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

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



Business-centric GRC

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

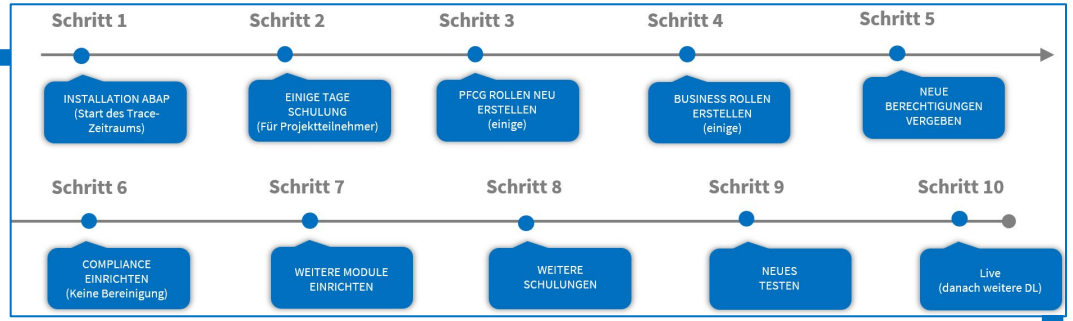
Bestehende Rollen werden bestmöglich genutzt

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

soterion

S/4 Rollen entschärfen oder neu generieren?

Welche Rollen bereiten Probleme?

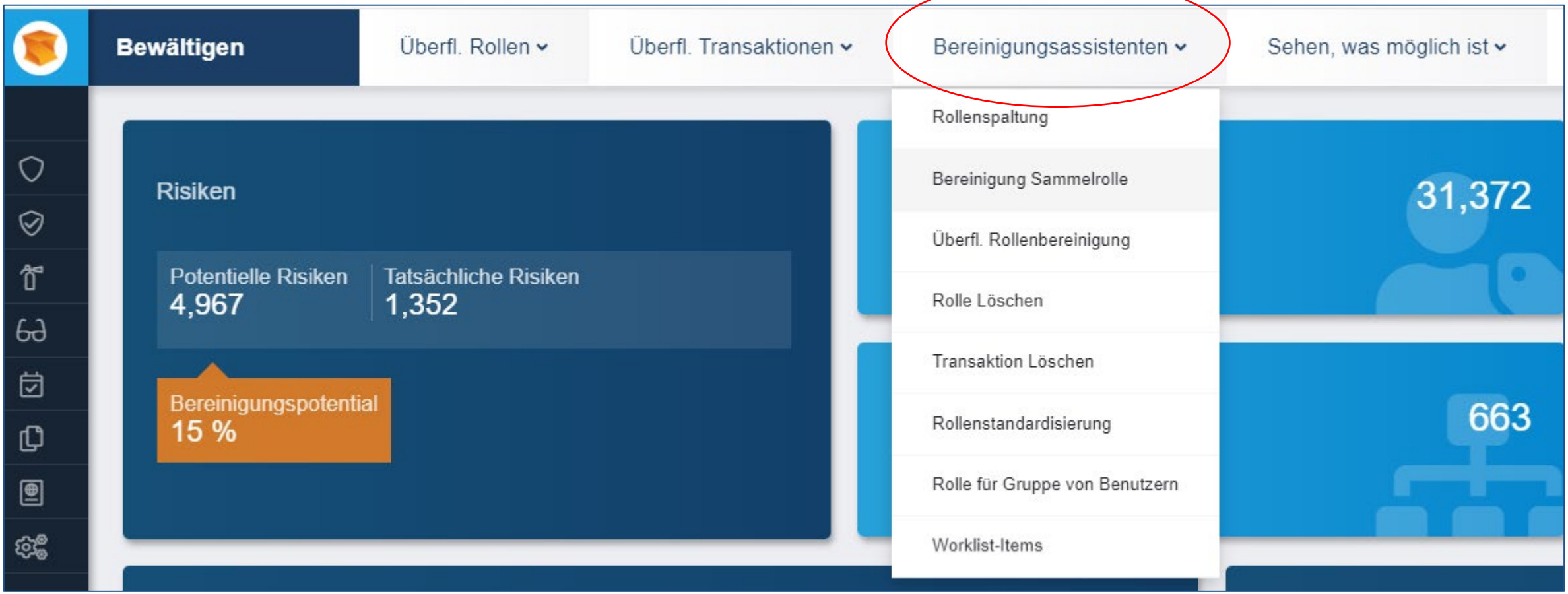
Zuerst neues S/4 Rollenset?

Ziel im S/4:

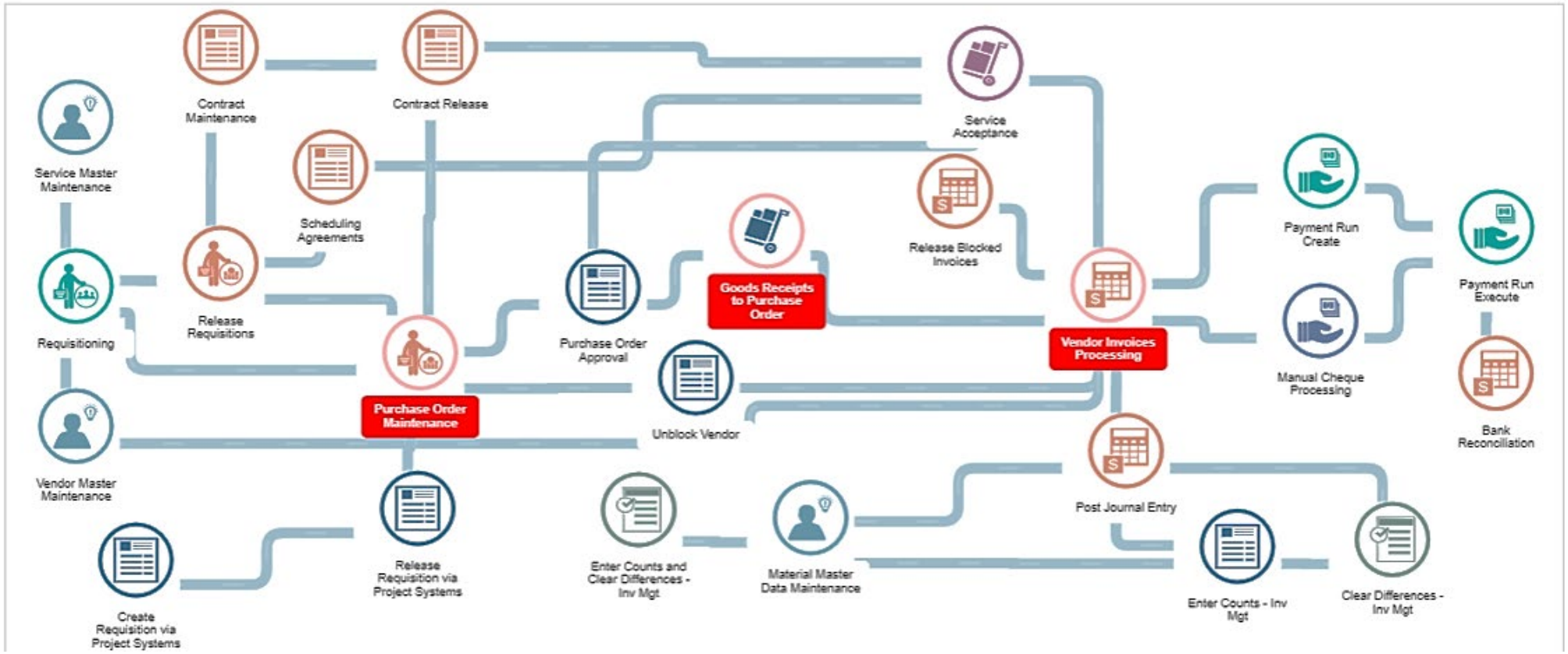
- **Sicheres System**
- **Einhaltung der Vorgaben**
- **Angemessener Aufwand in Relation zum Nutzen**

TIPP Nr.4:
Nutzen Sie Analyse-Tools für Ihre Rollen, um ein komplettes Re-Design möglichst zu vermeiden.

Beispiel Rollen Assistenten



S/4 Prozesse leicht verständlich

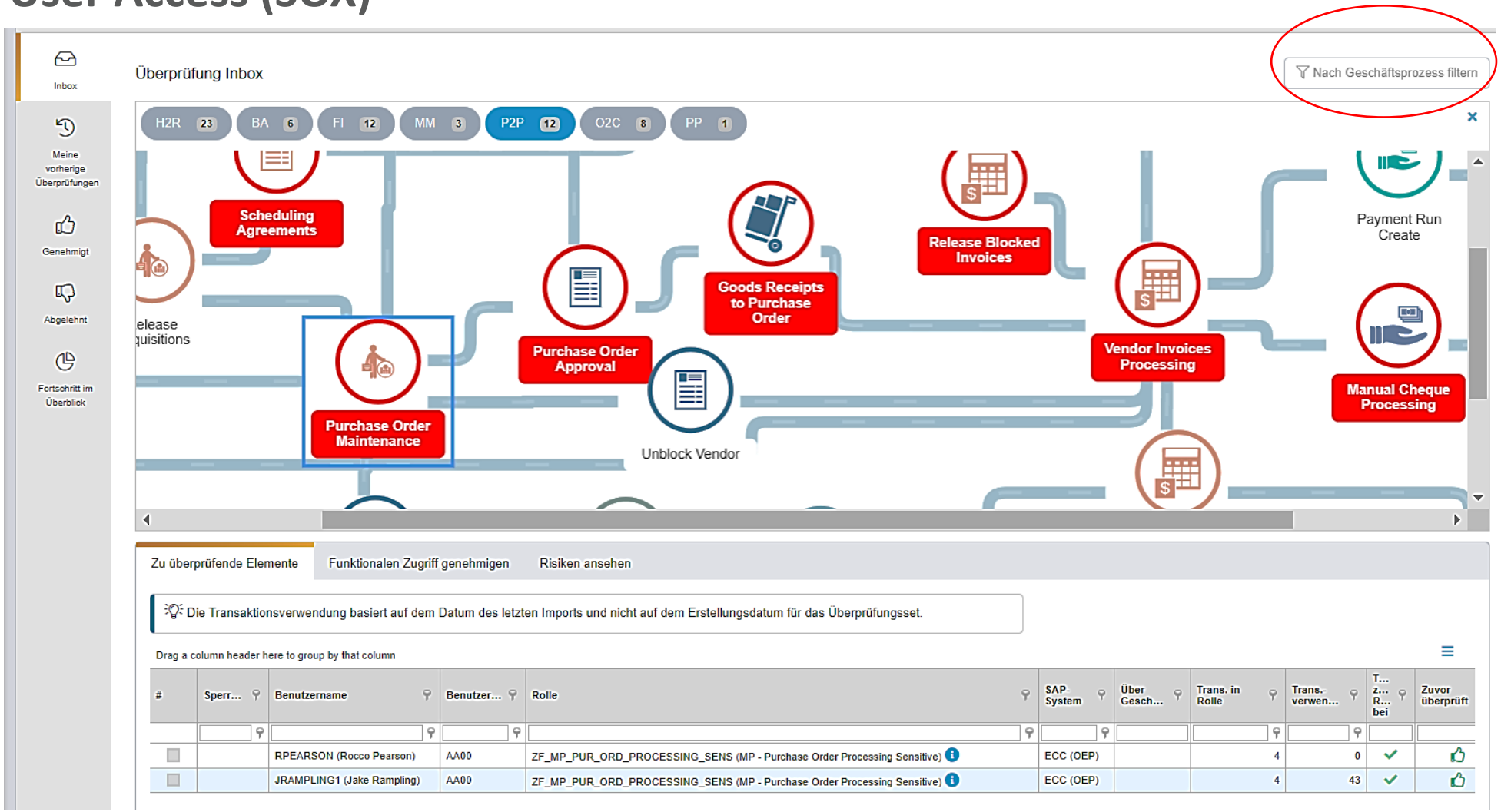


TIPP Nr.5:
Lassen Sie sich die Risiken visualisieren. So schaffen Sie die notwendige Risiko-Sensibilität im S/4.

soterion

Rezertifizierung User Access (SOX)

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



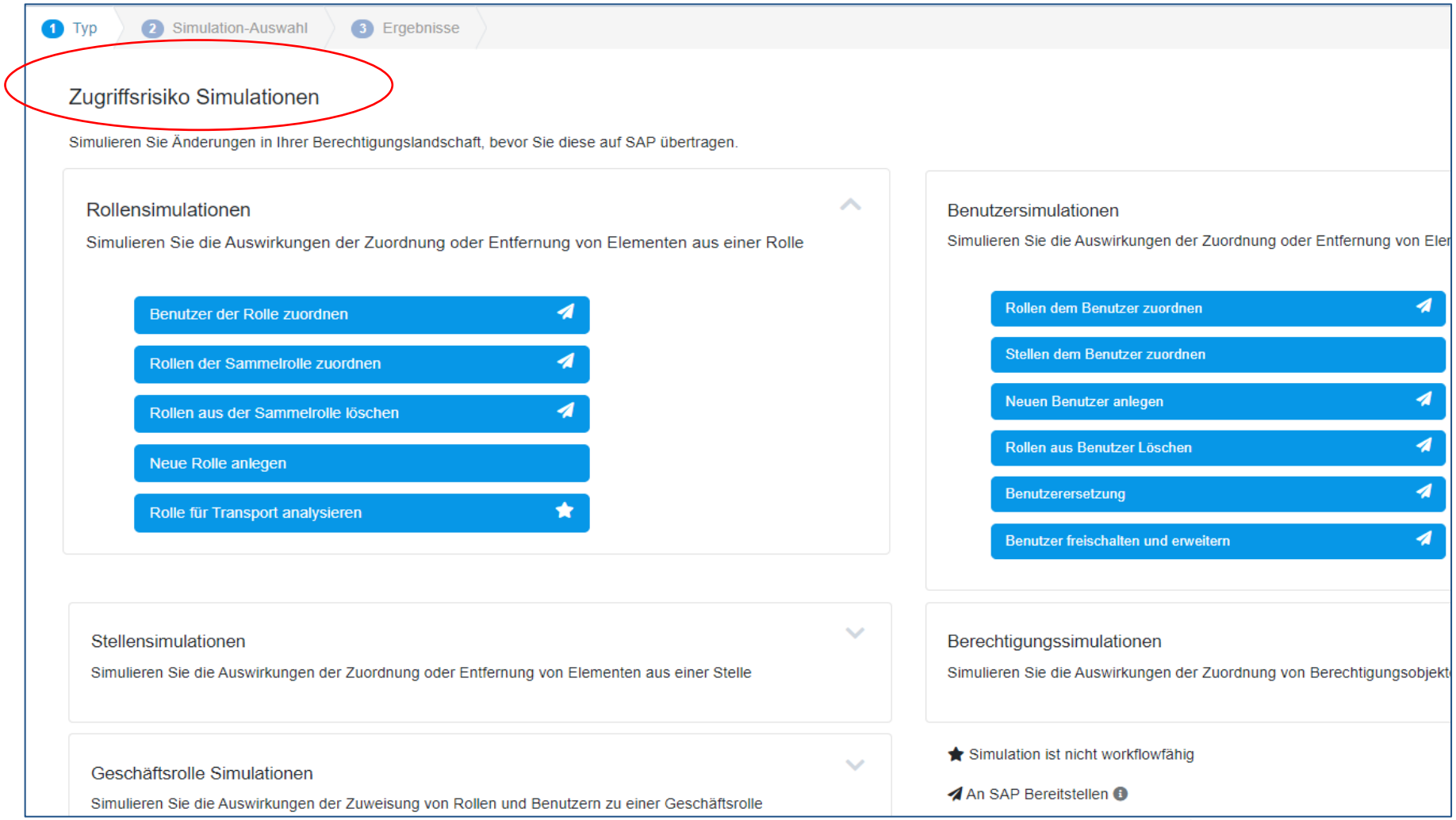
soterion

Out of the box Regelwerk auch für SuccessFactors

soterion

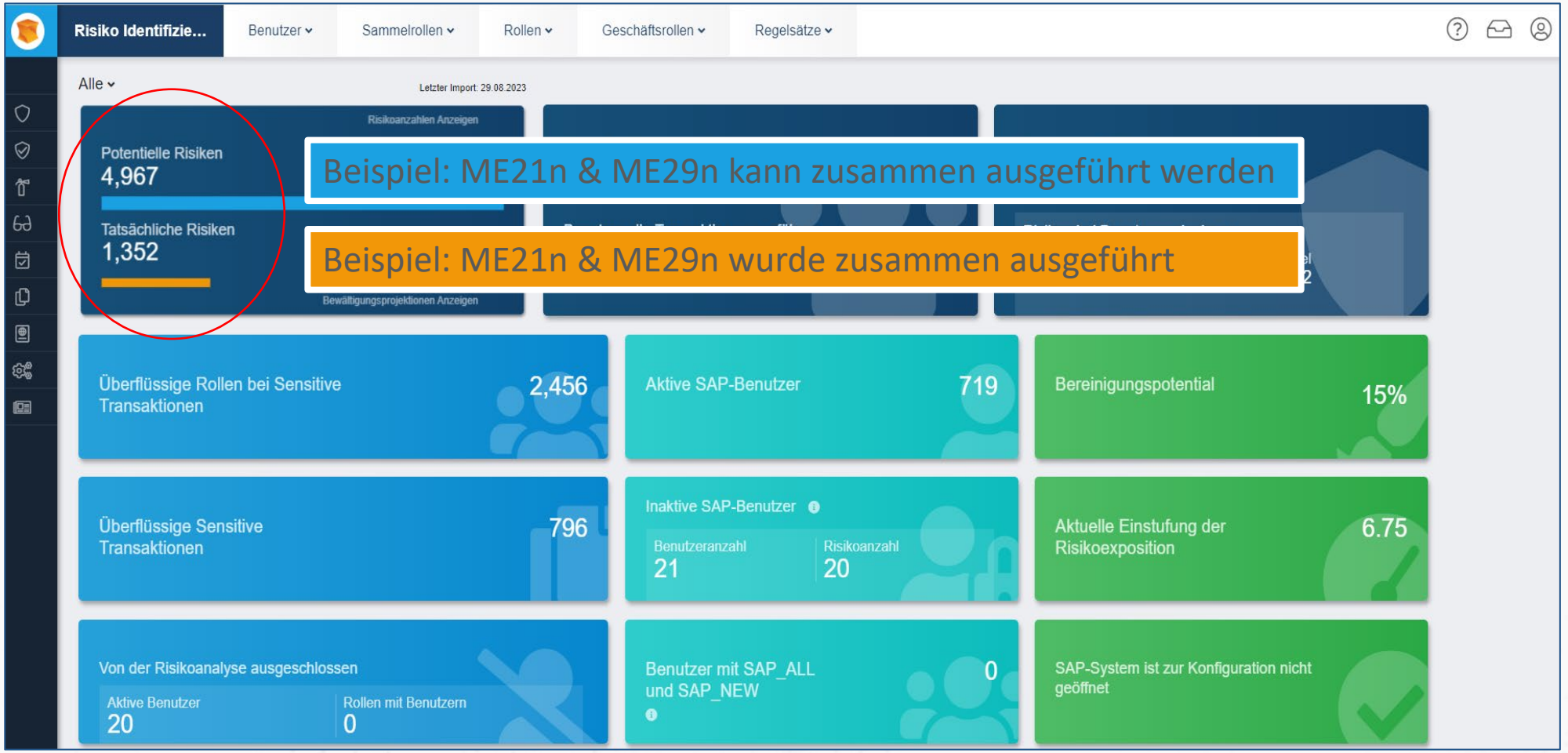
Simulationen verhindern Wildwuchs und überflüssige Workflows

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



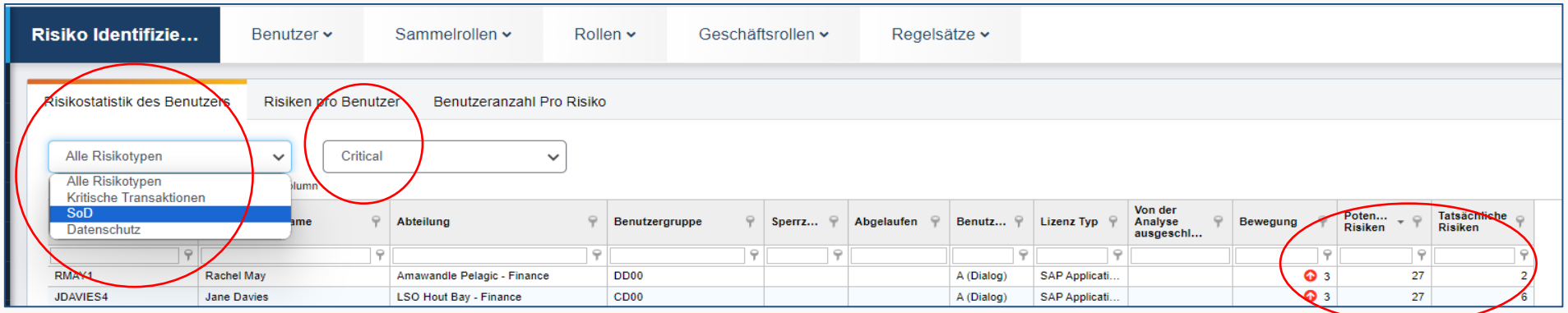
soterion

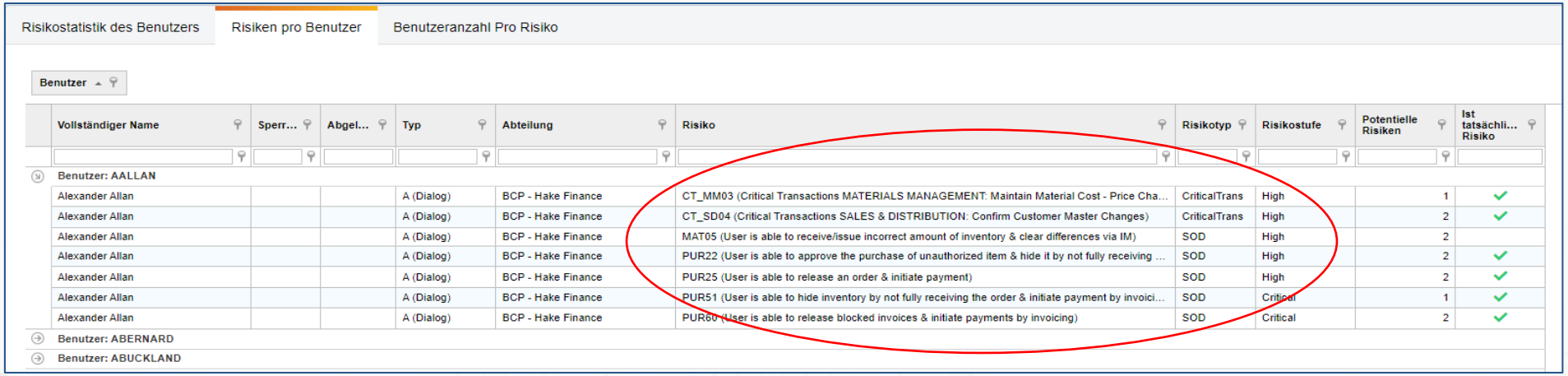
Risiko bzw. SoD Analysen von potenziellen und tatsächlichen Risiken



soterion

Risiko Analysen Details



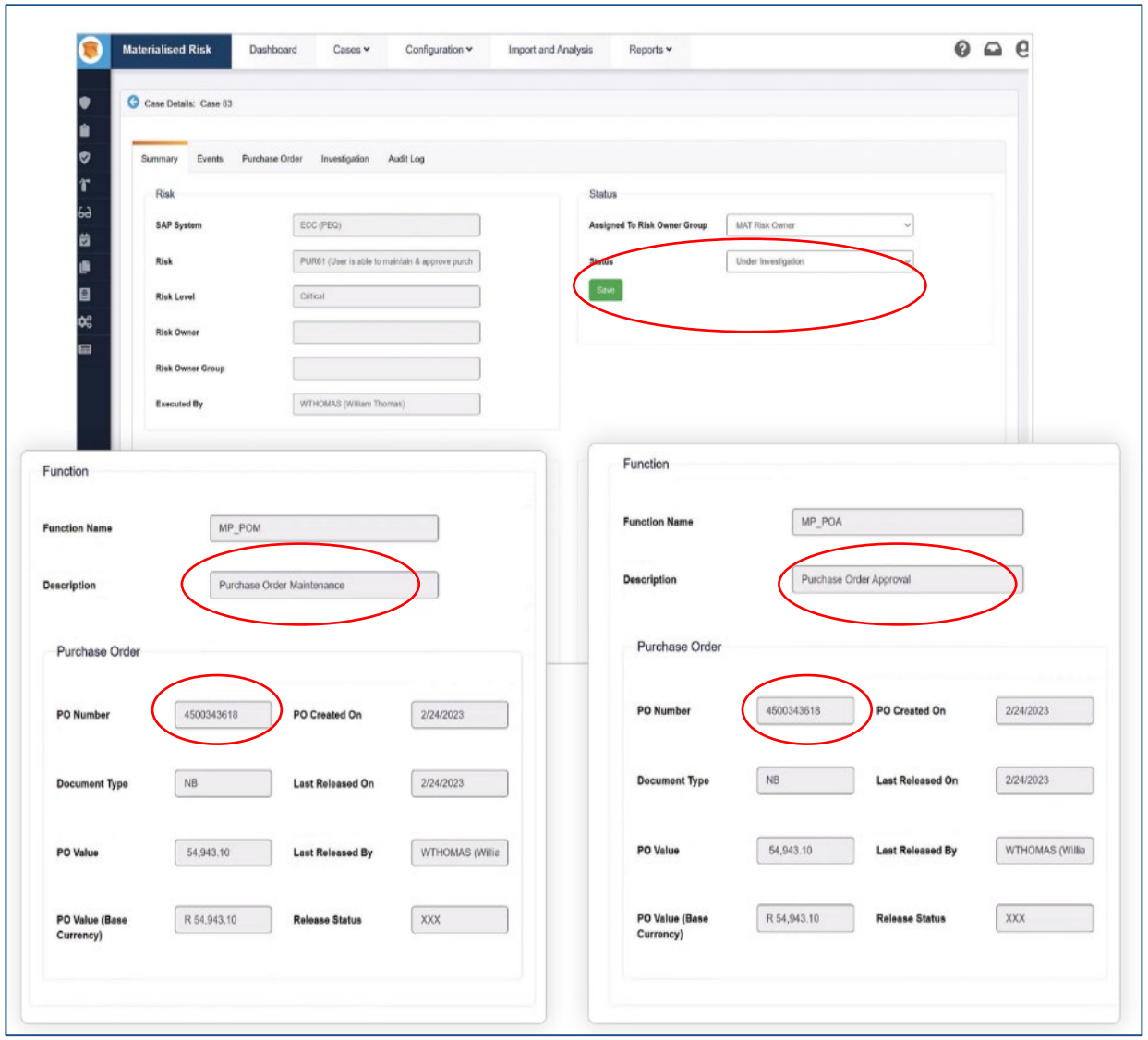


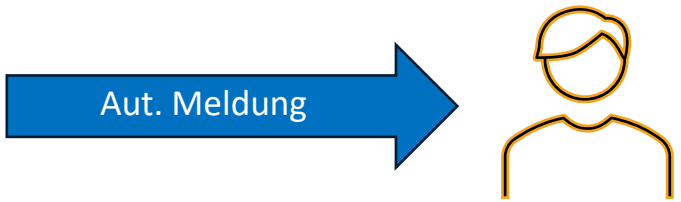
soterion

Mehr als nur SoD Analyse

SoD-Verstöße im Betrieb automatisch überwachen

Betrieb mit automatisierter SoD-Compliance (Prozesskontrolle)





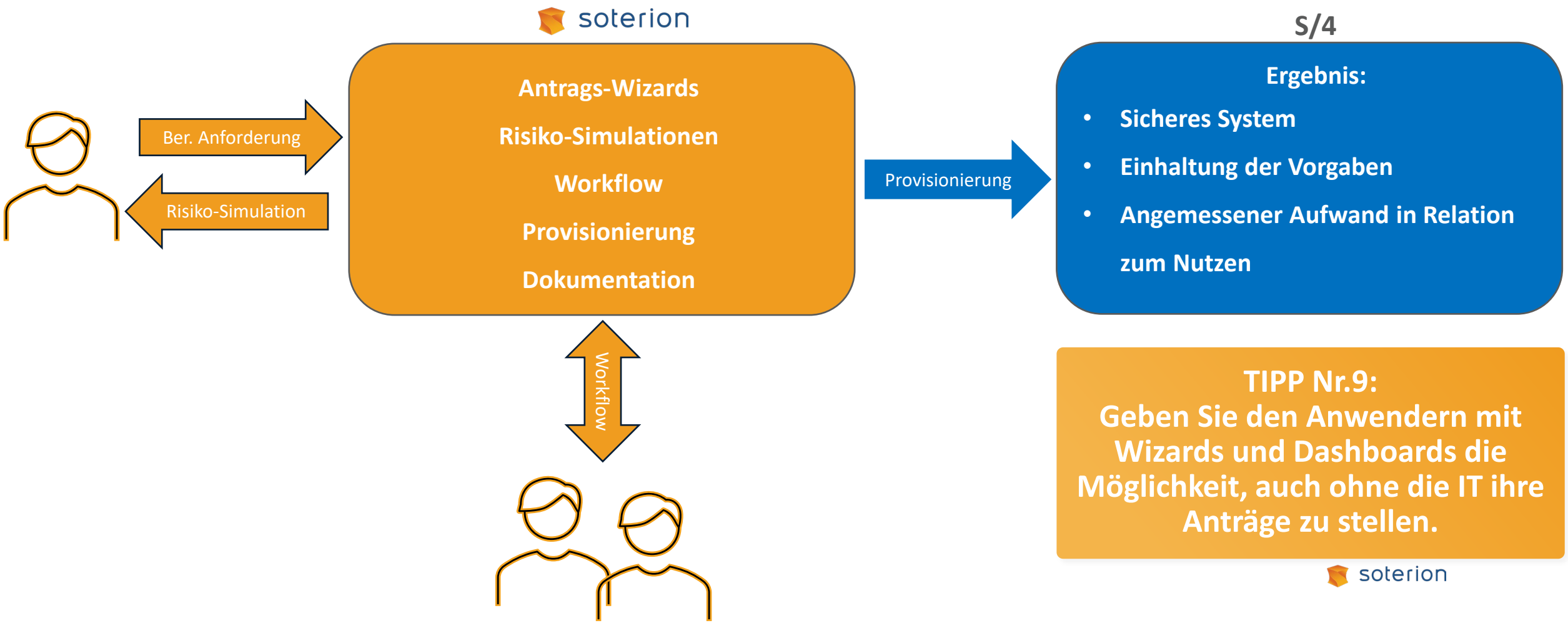
TIPP Nr.8:
Nutzen Sie automatisierte Systeme für die Kontrolle geschäftskritischer Prozesse.

soterion

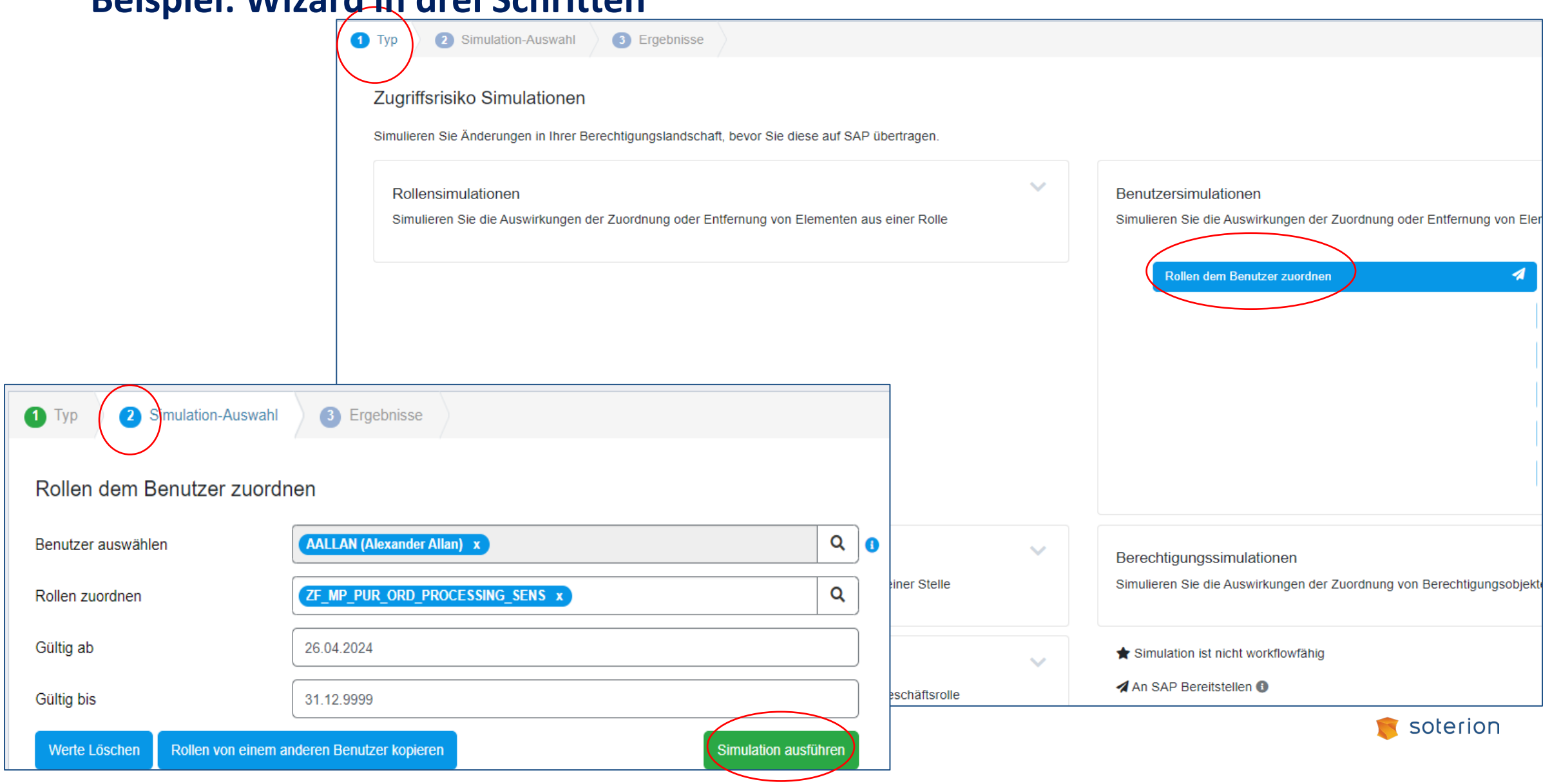
Was ist wichtig für den Fachbereich?

Sichere und verständliche Antrags- und Genehmigungsverfahren

Antrags- und Genehmigungsverfahren für Fachbereiche

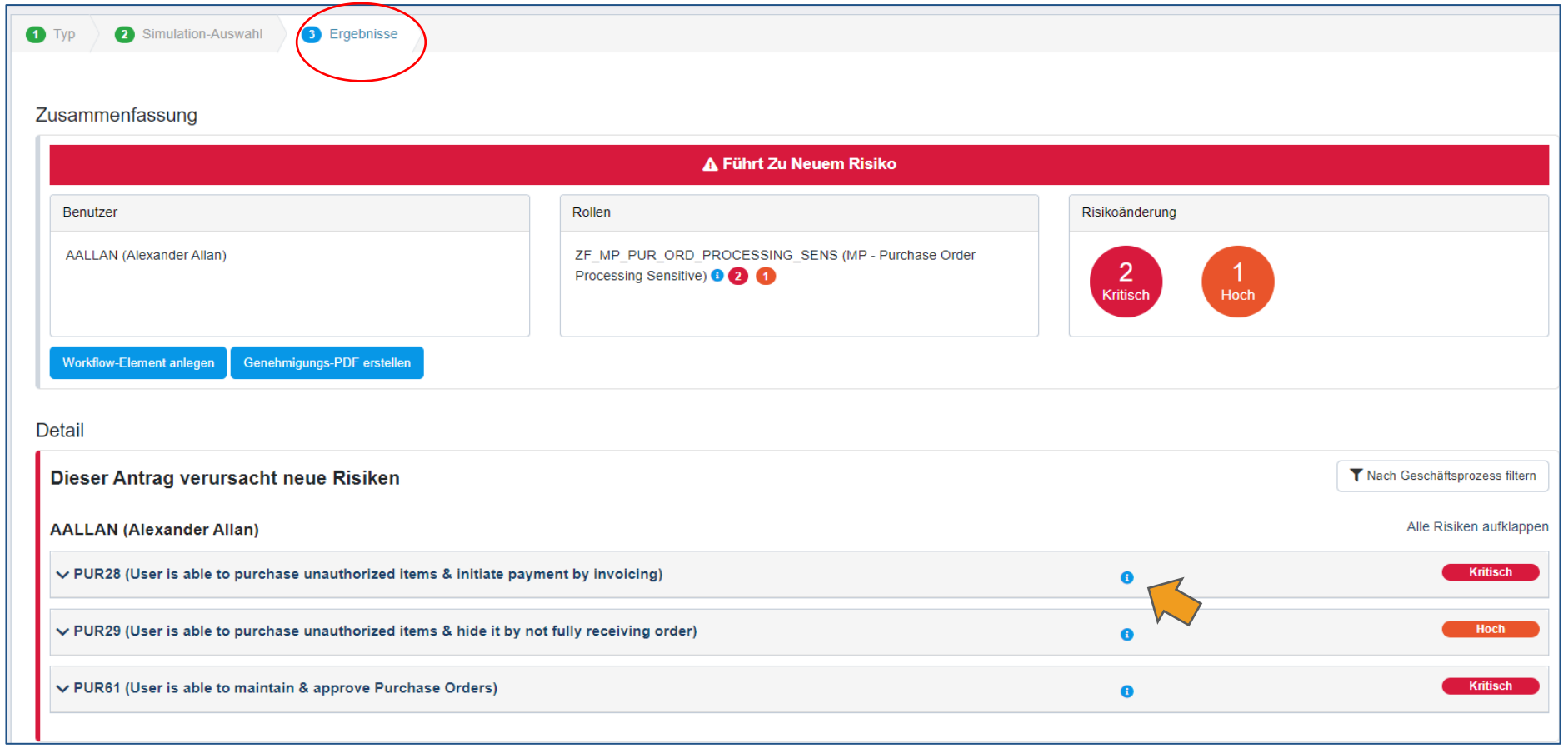


Beispiel: Wizard in drei Schritten



soterion

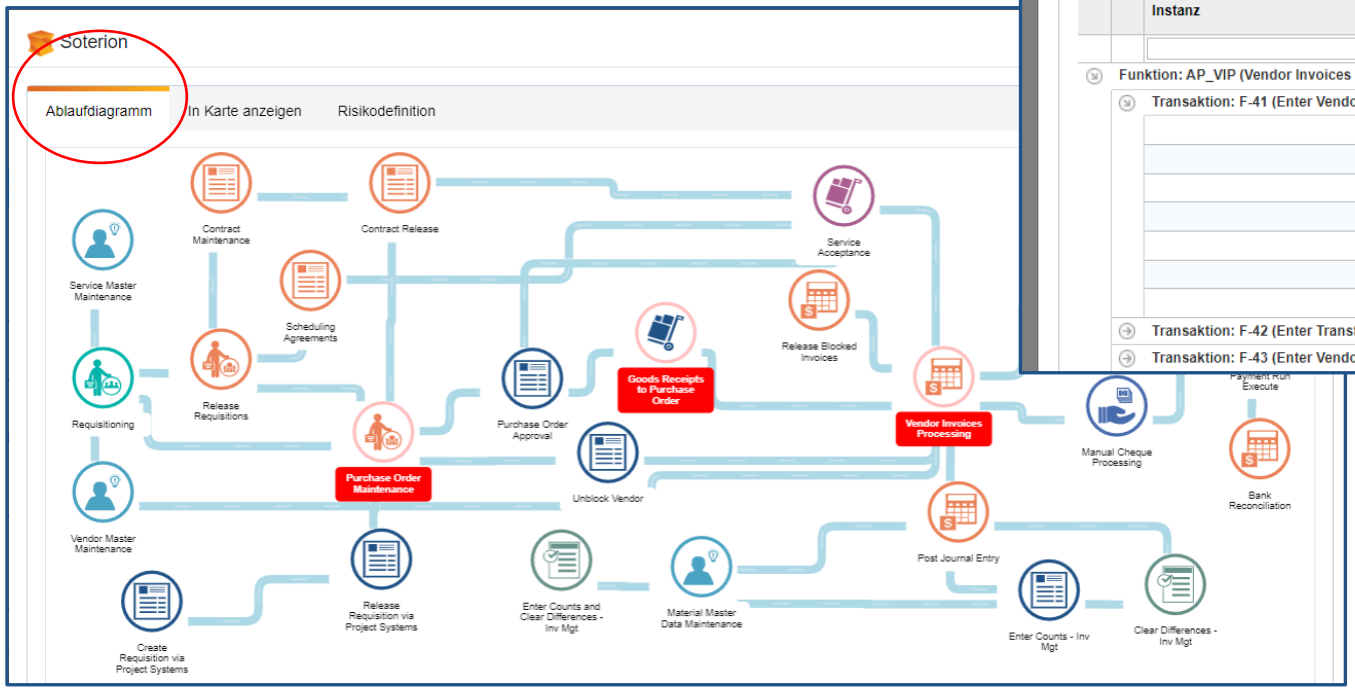
Beispiel: Wizard Ergebnis

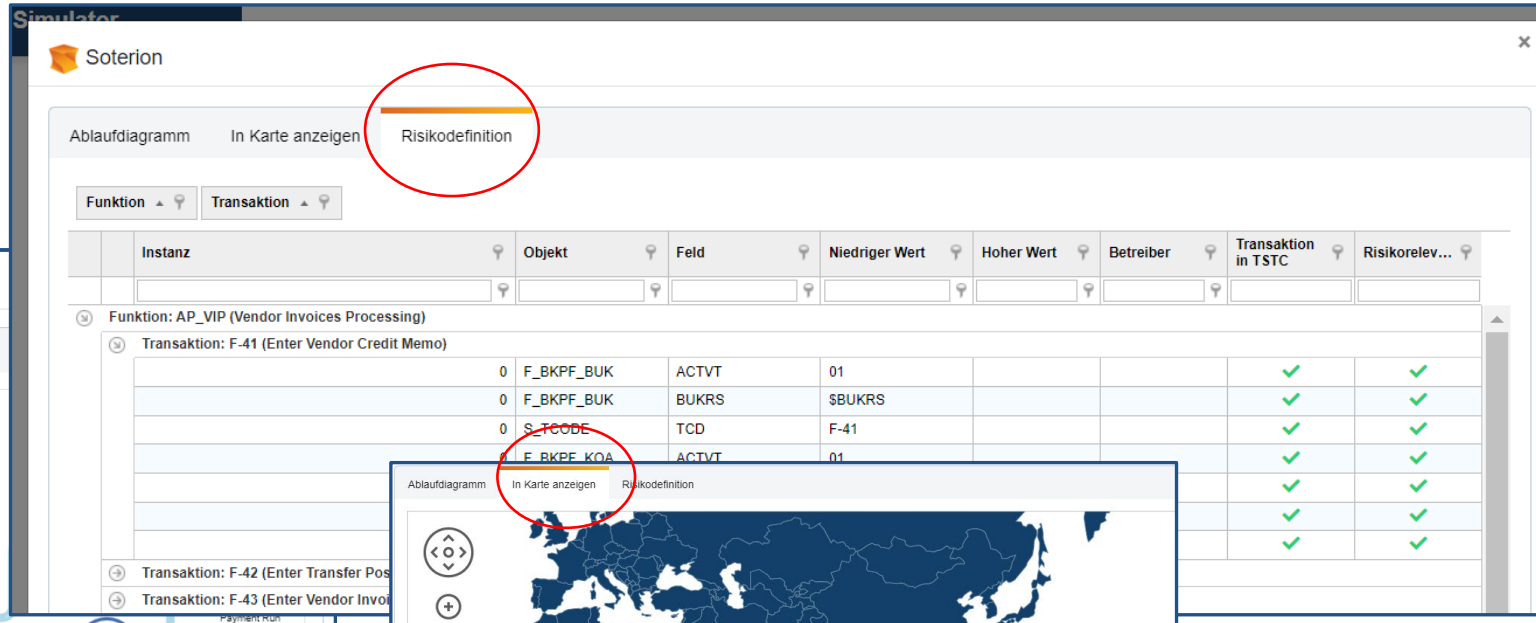


„Papierantrag“ via PDF oder Workflowantrag

soterion

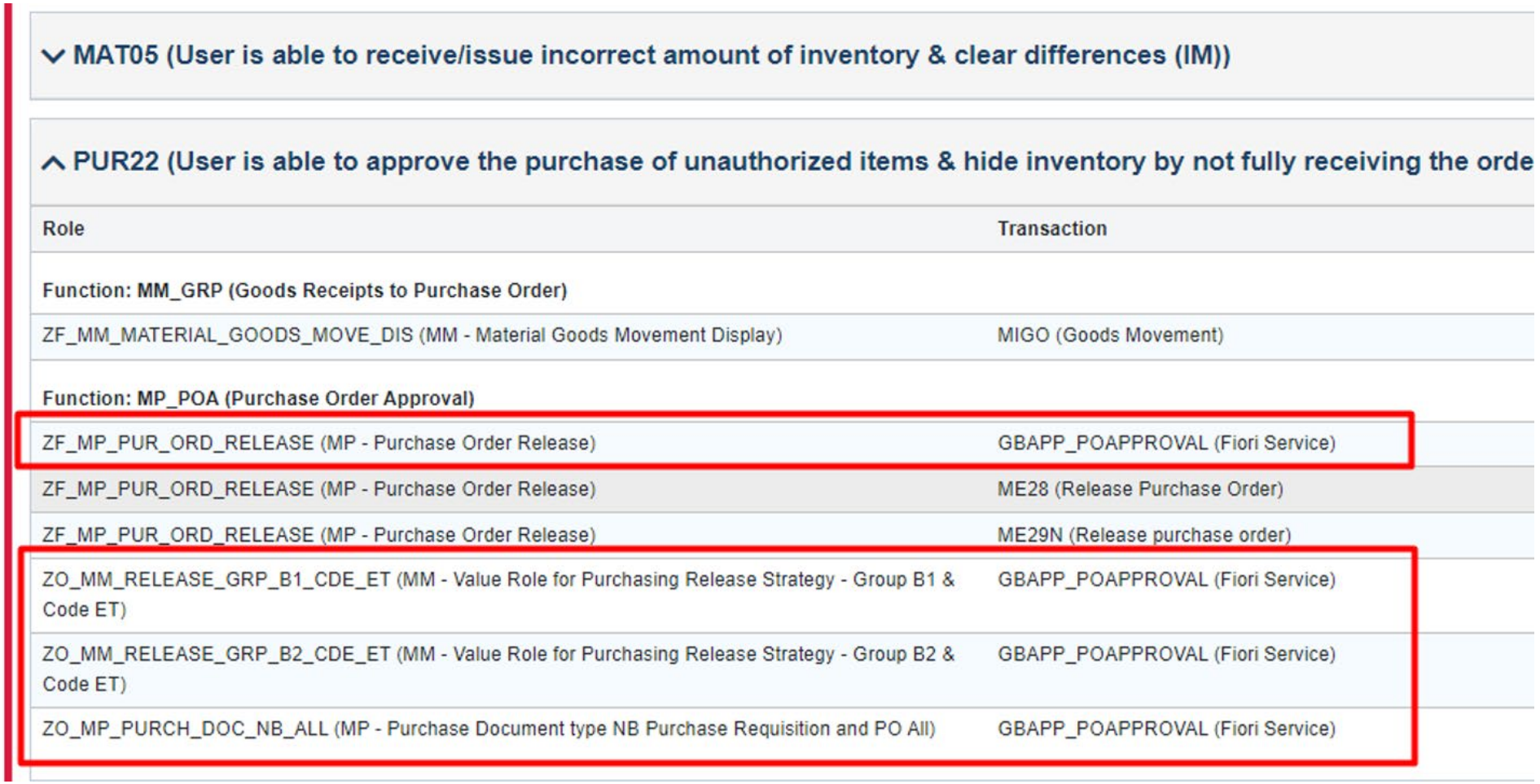
Wenn es der Antragsteller genau wissen will…PUR28





soterion

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 orde

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:

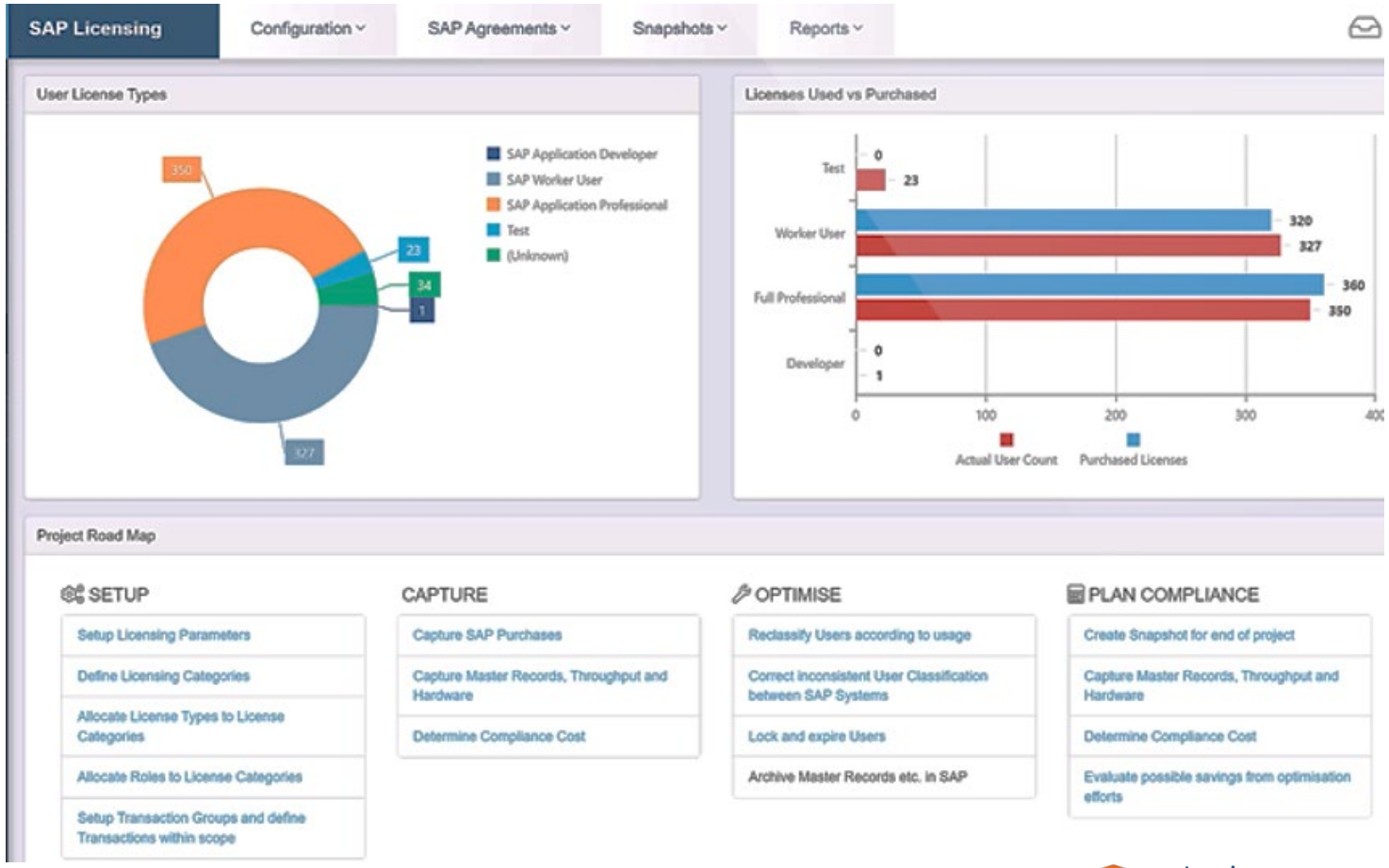
TIPP Nr.10:
Versuchen Sie ungeachtet der „Faktenlage“, Ihre Preise mit SAP zu verhandeln

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.

Eine Bitte in eigener Sache zum Thema SAP Star Analyse:

Unterstützen Sie uns bei der künftigen Lizenzierungs-Analyse.



soterion

Von Transaktionen zu Berechtigungsobjekten!

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?

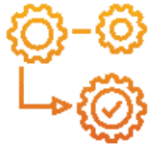
soterion

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 Risikobehebung, die durchgeführt werden könnten, um das Zugriffsrisiko der Organisation zu verringern.

soterion

Questions

Vielen Dank!

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