SAP Security Group Deutschland

Xiting Kunden-Event
mit Partnern

9./10.
MAI
2023

Risiko und Compliance Management mit der XAMS heute und morgen – die Cloud im Visier

Erik Trouillet | Olaf Sauer

Agenda

1. Heutige Anforderungen an ein GRC-Tool
2. Wie setze ich die XAMS als GRC-Tool ein
3. Der nächste Schritt: GRC in der Cloud
4. Roadmap: Ein Ausblick

Kapitel 1

Heutige Anforderungen an ein GRC-Tool

Was weiss ChatGPT über GRC?

ET Was sind die Anforderungen an ein GRC Tool?

Ein GRC-Tool (Governance, Risk, and Compliance-Tool) ist ein Software-Tool, das Unternehmen bei der Verwaltung und Überwachung von Governance-, Risiko- und Compliance-Aktivitäten unterstützt. Die Anforderungen an ein GRC-Tool können je nach Unternehmen und Branche unterschiedlich sein, aber im Allgemeinen sollten GRC-Tools folgende Funktionen und Eigenschaften haben:

- Governance-Unterstützung
- Risikomanagement
- Compliance-Management
- Reporting- und Analysefähigkeiten
- Benutzerfreundlichkeit
- Integration
- Sicherheit
- Skalierbarkeit

Quelle: OpenAI ChatGPT

Herausforderungen an die Sicherheit durch komplexe hybride Landschaften

Einheitliche Sicherheitsarchitektur für hybride Landschaften

- Einheitliche Konzepte
- Einheitliches Identitäten- und Berechtigungsmanagement
- Cross-System Segregation of Duties (auch Non-SAP)
- Einheitliches Security Monitoring
- Einheitlicher Umgang mit Threats

Kapitel 2

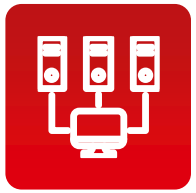
Wie setze ich die XAMS als GRC-Tool ein

GRC Funktionen in der XAMS und XCW

Regelwerk

Analyse

Role Management



User Management

Rezertifizierung & Betrieb

SAP Cloud Identity Access Governance

SAP GRC Access Control

SAP Cloud Identity Access Governance

SAP GRC Access Control

SAP Identity Management

XAMS

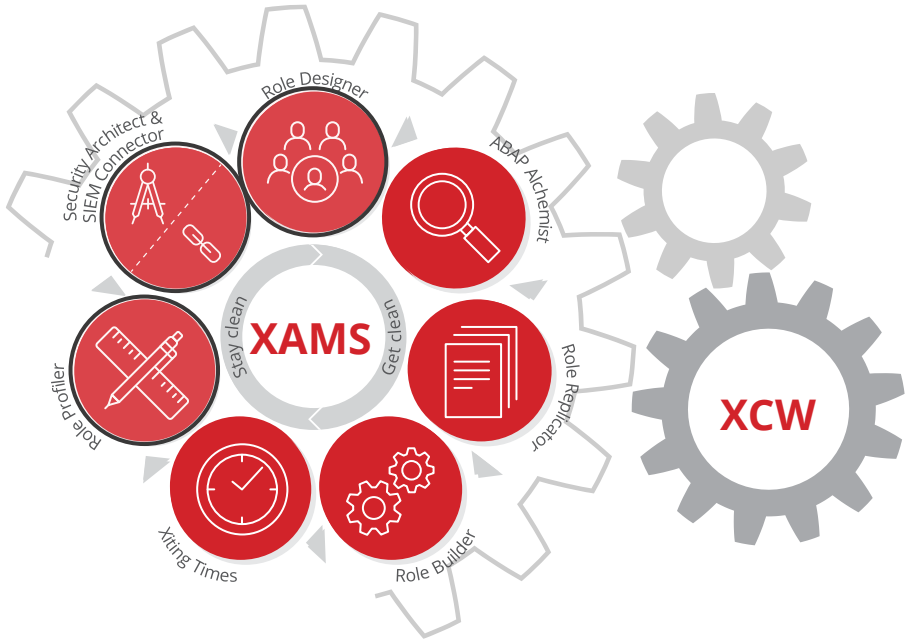
XCW

XAMS

Risikoanalyse mit XAMS CRAF

Critical Authorization Framework

Das CRAF ist die Schaltzentrale der XAMS, welche Prüfungsmöglichkeiten zu jeder Zeit erlaubt.



XAMS CRAF ist in mehreren XAMS Modulen nativ integriert:

1. Role Designer für die Prüfung von virtuellen Rollen noch vor Erstellung in PFCG

2. Role Profiler zur Qualitätssicherung (Adhoc Analysen)

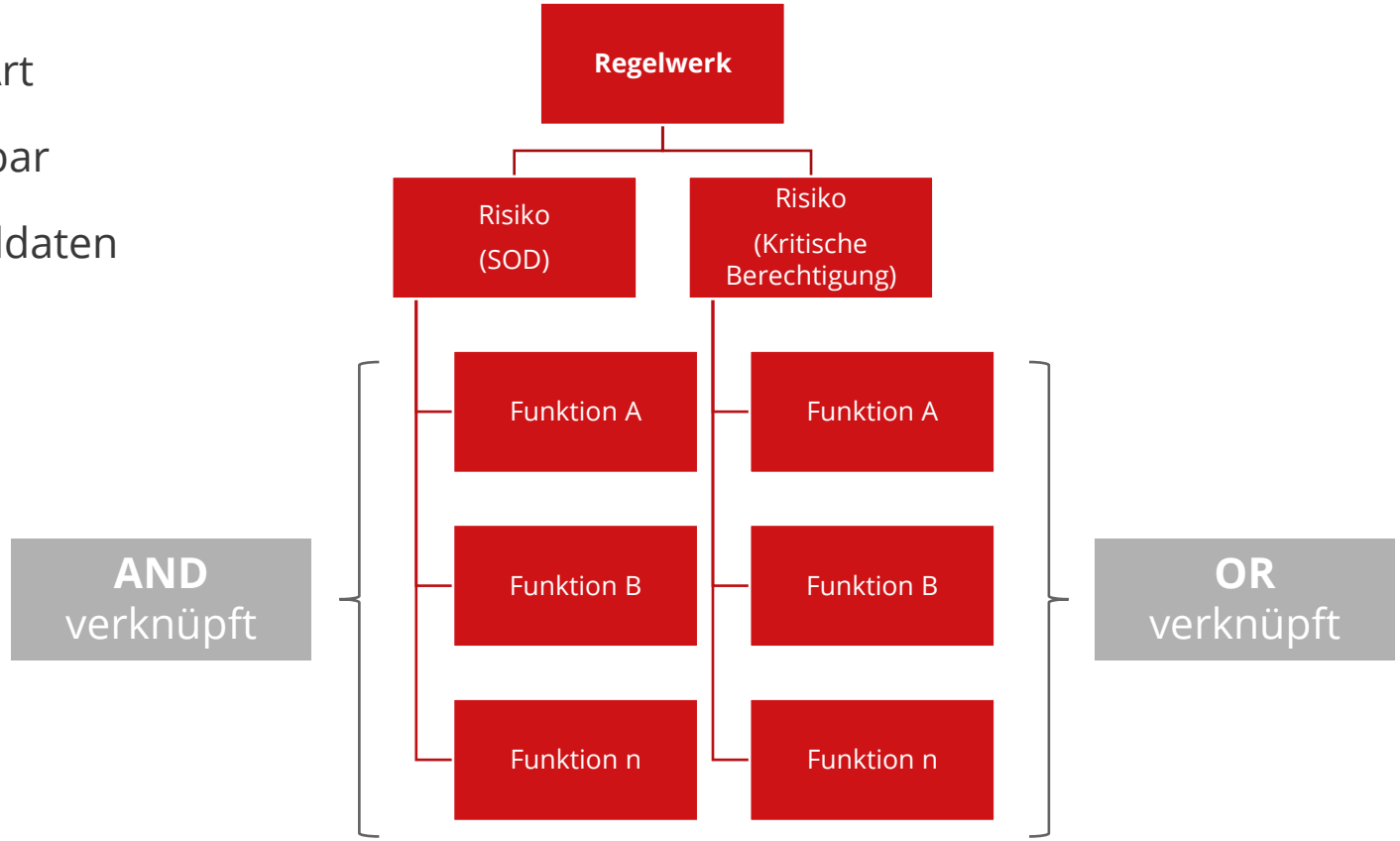
3. Security Architect für regelmässige Risikoanalysen (Controls Monitoring)

Sowie im “SAP Standard” bei Bedarf:

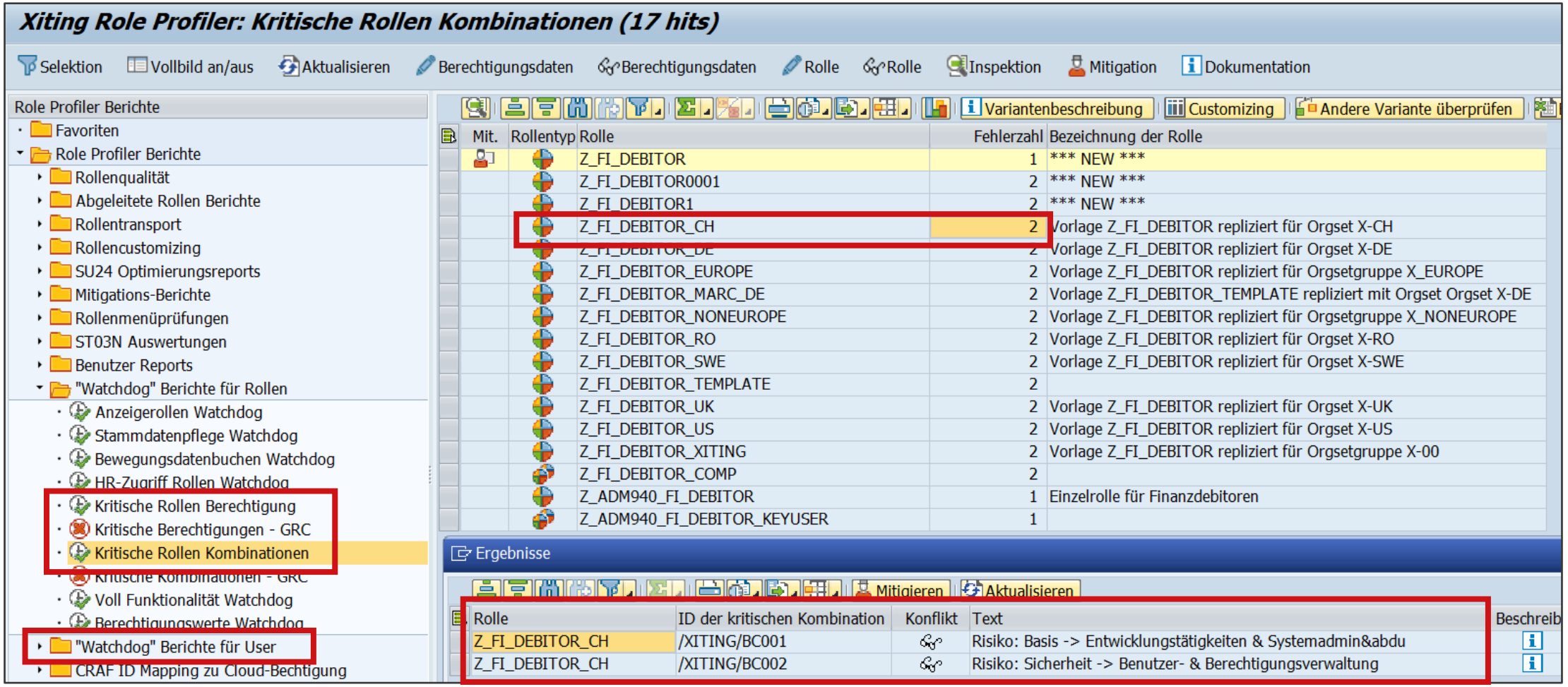
4. PFCG zur Direktprüfung bei Rollenänderungen

Critical Authorizations Framework

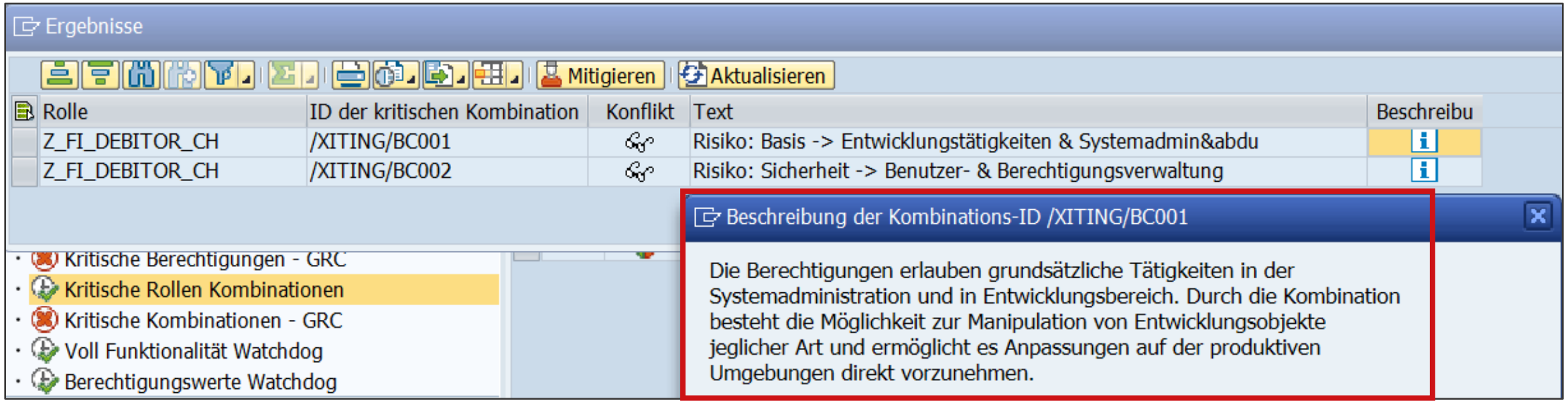
- Zentrales Prüfungs-Framework in der XAMS
- Risikoanalyse mit Hilfe von Regeln jeder Art
- Jede Komplexität ist bei den Regeln denkbar
- Prüfungsgrundlage sind Rollen- und Profildaten
- Zentrale Überwachungsmöglichkeiten
- Vielseitige Integration
- Mitigationsframework



SOD Prüfung auf Ebene Rollen und / oder Benutzer



Qualitative Beschreibung des SOD Konflikts



Technische Darstellung des SOD Konflikts

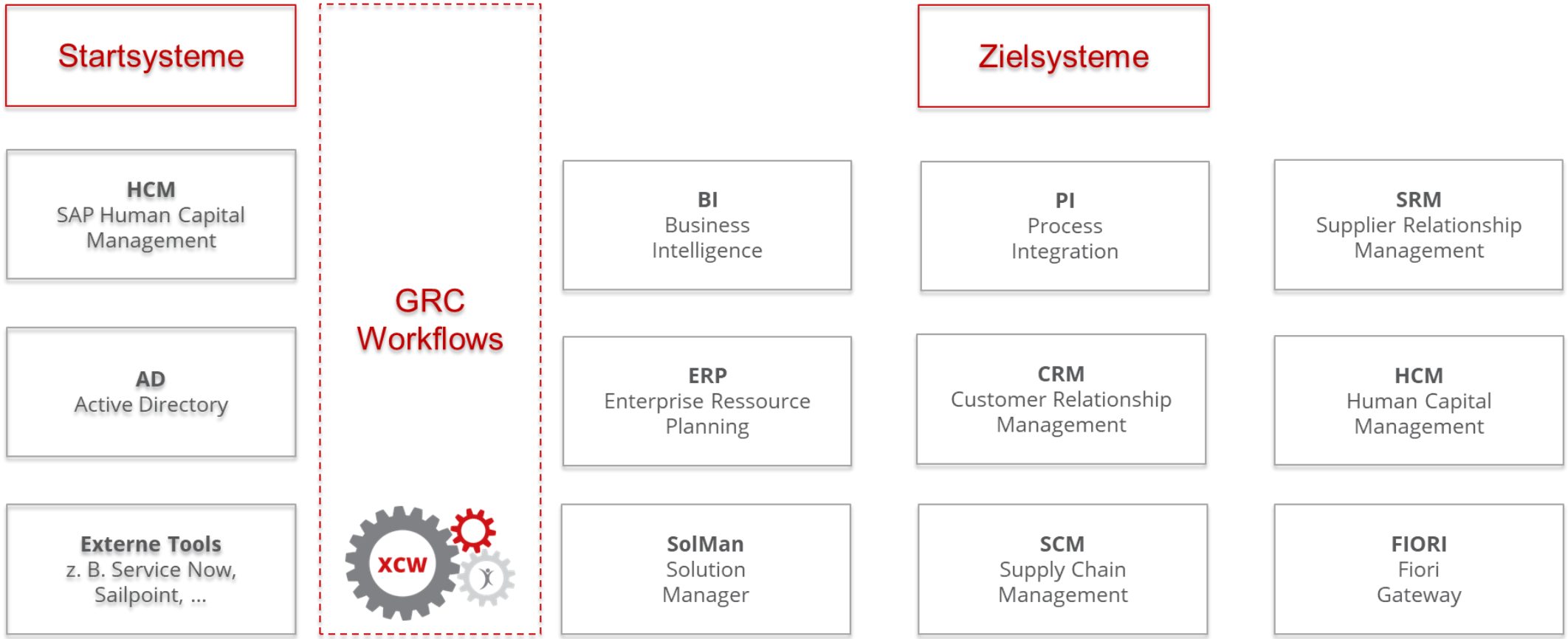
Konflikte

Rollenobjekt	Rollenauth.	Rollenfeld	Rolle-Von	Rolle-Bis	Status	Verwend.	Obj.Wer...	AuthID	Grup...
S_DEVELOP	T-XT6011970...	ACTVT	01					/XITING/BC_ADM1	ORG2
S_DEVELOP	T-XT6011970...	ACTVT	02					/XITING/BC_ADM1	ORG2
S_DEVELOP	T-XT6011970...	OBJTYPE	FUGR					/XITING/BC_ADM1	ORG2
S_RFC_ADM	T-XT6011970...	ACTVT	01					/XITING/BC_ADM2	OR1
S_RFC_ADM	T-XT6011970...	ACTVT	02					/XITING/BC_ADM2	OR1
S_RFC_ADM	T-XT6011970...	ACTVT	06					/XITING/BC_ADM2	OR1
S_USER_GRP	T-XT6011970...	ACTVT	06					/XITING/BC_ADM2	OR1
S_USER_GRP	T-XT6011970...	ACTVT	06					/XITING/BC_ADM2	OR1

Beschreibung der Kombinations-ID /XITING/BC001

Die Berechtigungen erlauben grundsätzliche Tätigkeiten in der Systemadministration und in Entwicklungsbereich. Durch die Kombination besteht die Möglichkeit zur Manipulation von Entwicklungsobjekte jeglicher Art und ermöglicht es Anpassungen auf der produktiven Umgebungen direkt vorzunehmen.

Workflows für die Provisionierung / Entzug von Berechtigungen



Workflows für die Provisionierung / Entzug von Berechtigungen (Fortsetzung)

Benutzeranlage/-änderung

- Erstellung einer neuen SAP-Benutzerkennung
- Änderung einer bestehenden SAP-Benutzerkennung

Rollenvergabe/-entzug

- Zuweisung einer Rolle zu einer SAP- Benutzerkennung
- Entzug einer Rolle von einer SAP-Benutzerkennung

Benutzeranlage inkl. Rollenvergabe

- Erstellung einer neuen SAP-Benutzerkennung inkl. Zuweisung von Rollen

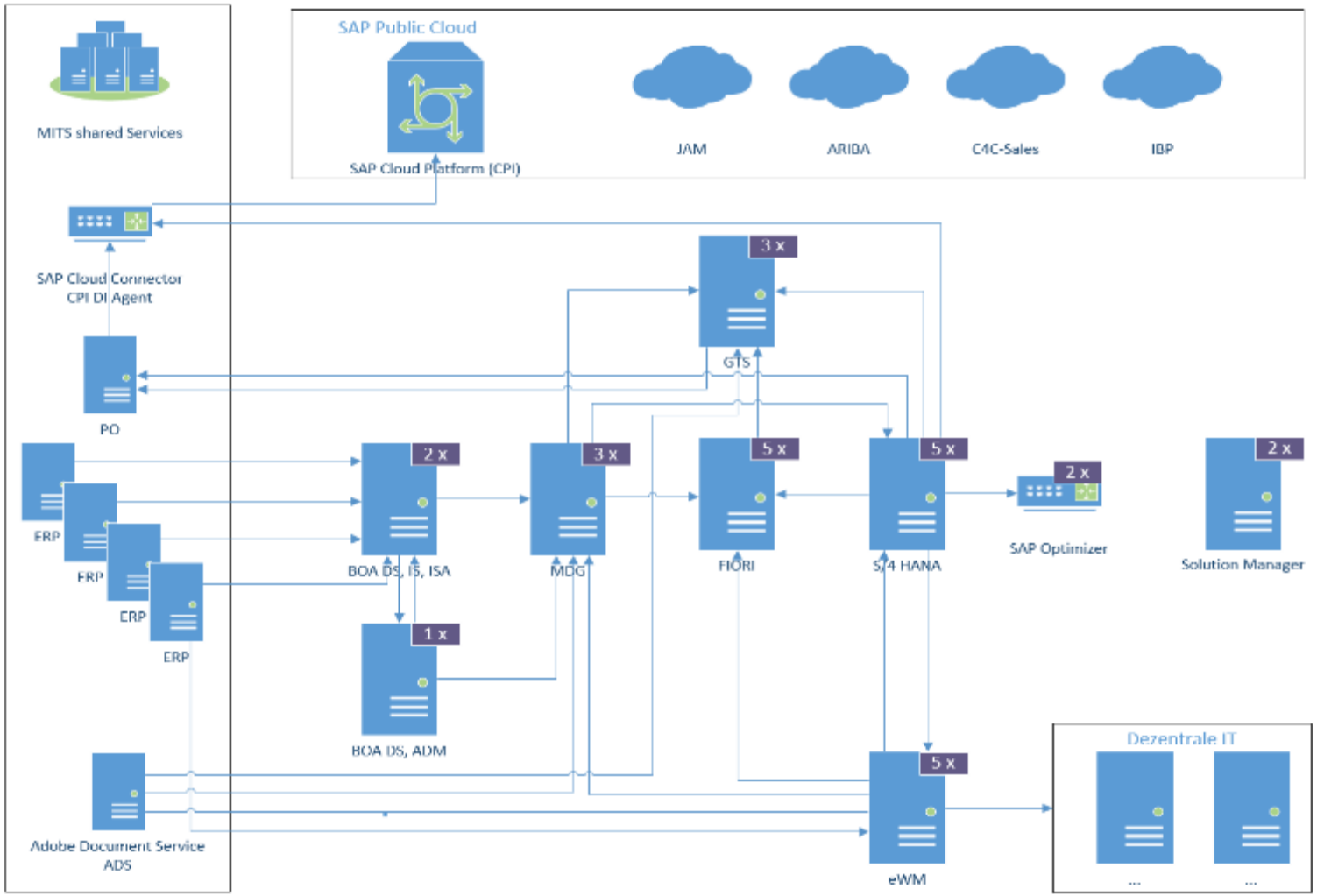
Erfüllung der GRC Anforderungen mit der XAMS

- Die XAMS hat ihre Stärken im SAP Berechtigungsmanagement und nutzt diese für sämtliche GRC Funktionen.

Kapitel 3

Der nächste Schritt: GRC in der Cloud

Komplexe hybride Landschaft Kundensicht



Cloud

On-premise

Komplexe hybride Landschaft SAP-Sicht

SaaS

- SAP SuccessFactors
- SAP S/4HANA Cloud
- SAP C/4HANA
- SAP Fieldglass
- SAP Concur
- SAP Ariba

Diese Produkte werden in der Cloud bereitgestellt und sind als Software as a Service (SaaS) verfügbar, sodass Sie auf Ihre Software von jedem Webbrowser aus zugreifen können.

EXTEND
Cloud & On-Prem Apps

EXPERIENCE
People & Data

BUILD
Differentiating Digital Apps

INTEGRATE
Apps, Data & Processes

PaaS

RUN WITH
- SAP®
- Customer Apps
- Partner Apps
- 3rd Party

INTERGRATE

Apps, Data, and Prozesse **ausserhalb der SAP Business Technology Platform**

RUN ON
SAP® Business Technology Platform

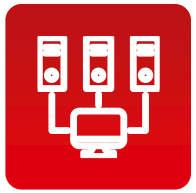
- SAP® Neo
- CLOUD FOUNDRY
- ABAP
- Kyma
- kubernetes
- SAP®
- aws
- Microsoft Azure
- Google Cloud
- Alibaba Cloud

GRC Funktionen aus der Cloud, für die Cloud, in der Cloud

Regelwerk

Analyse

Role Management



User Management

Rezertifizierung & Betrieb

SAP Cloud Identity Access Governance

SAP GRC Access Control

SAP Cloud Identity Access Governance

SAP GRC Access Control

SAP Identity Management

XAMS

XSP

XSP (Business Roles)

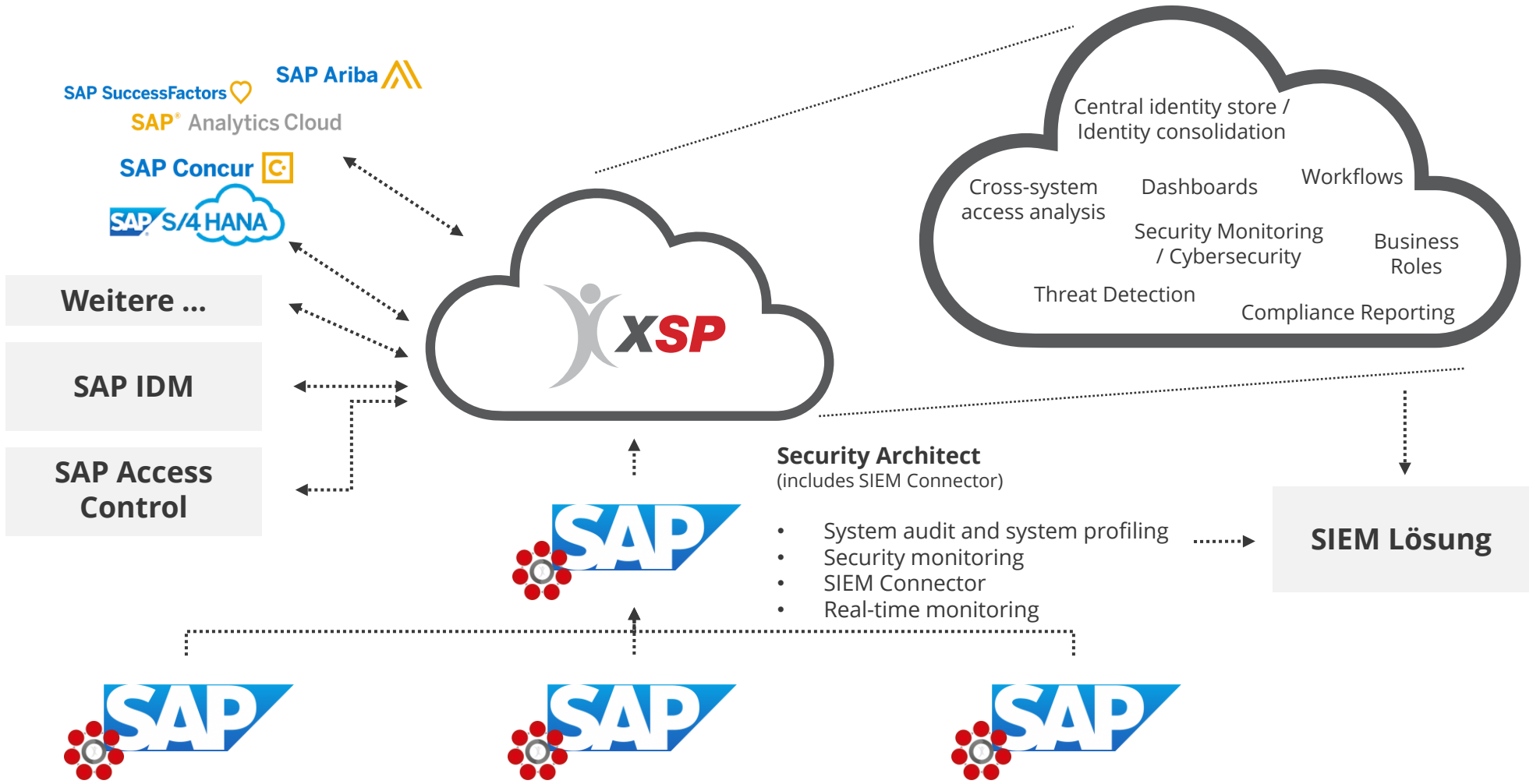
XCW

XAMS

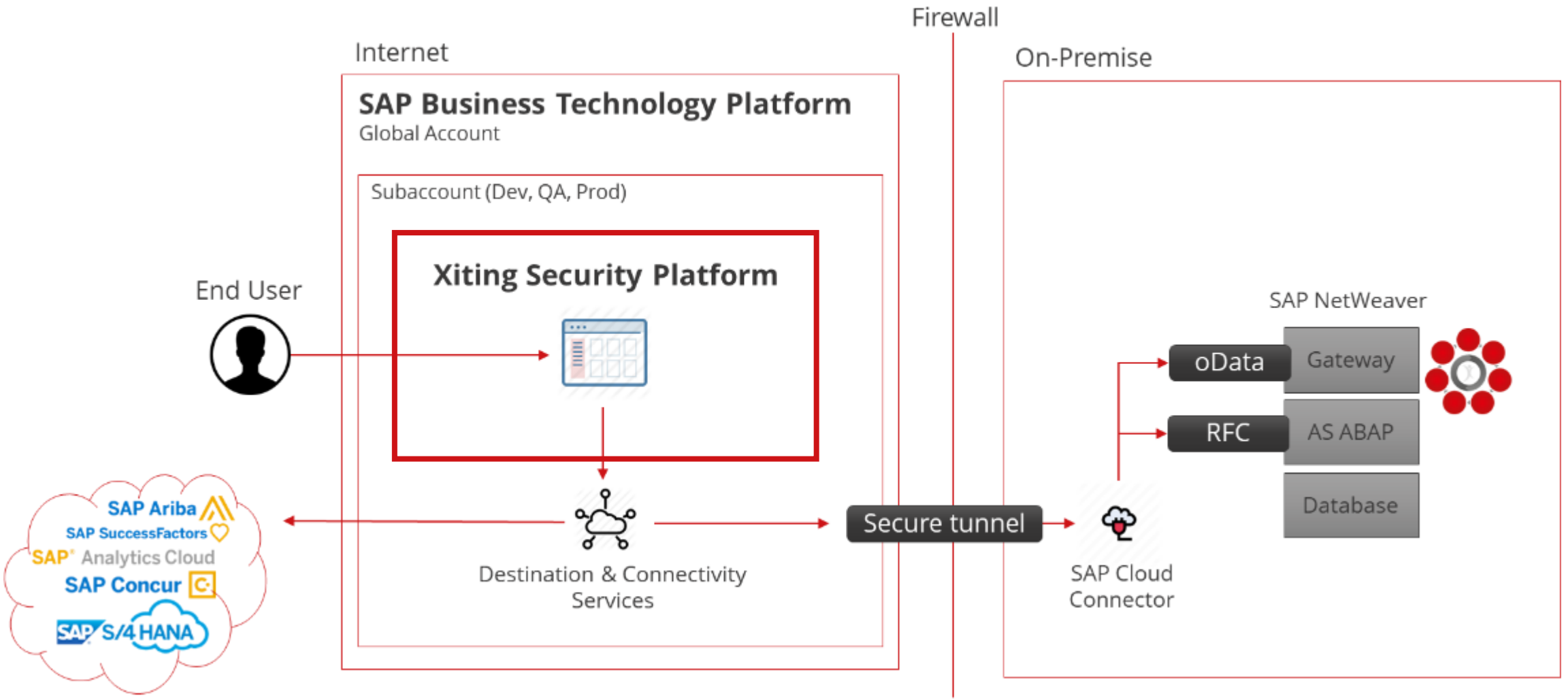
XSP

XSMS (XAMS, XCW, XSP)

Die XSP als Single Point of Truth



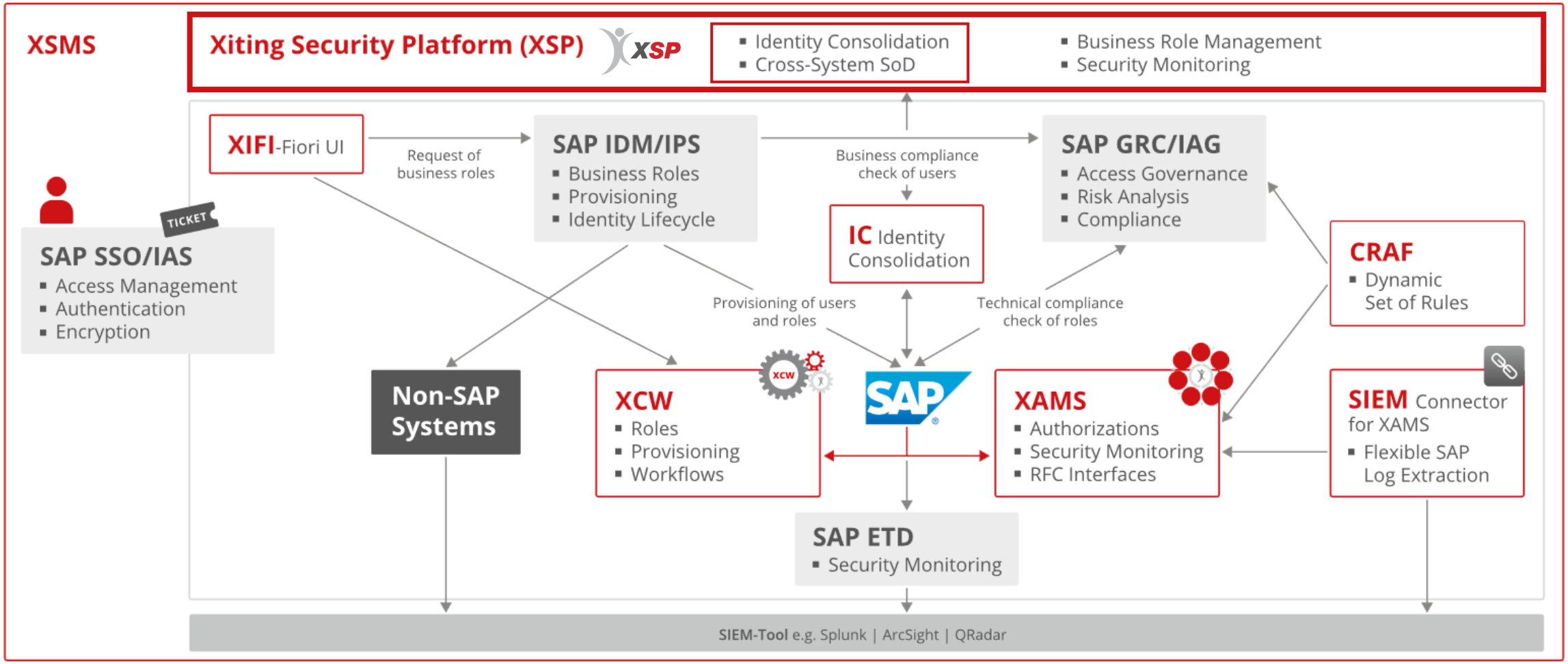
XSP Architektur



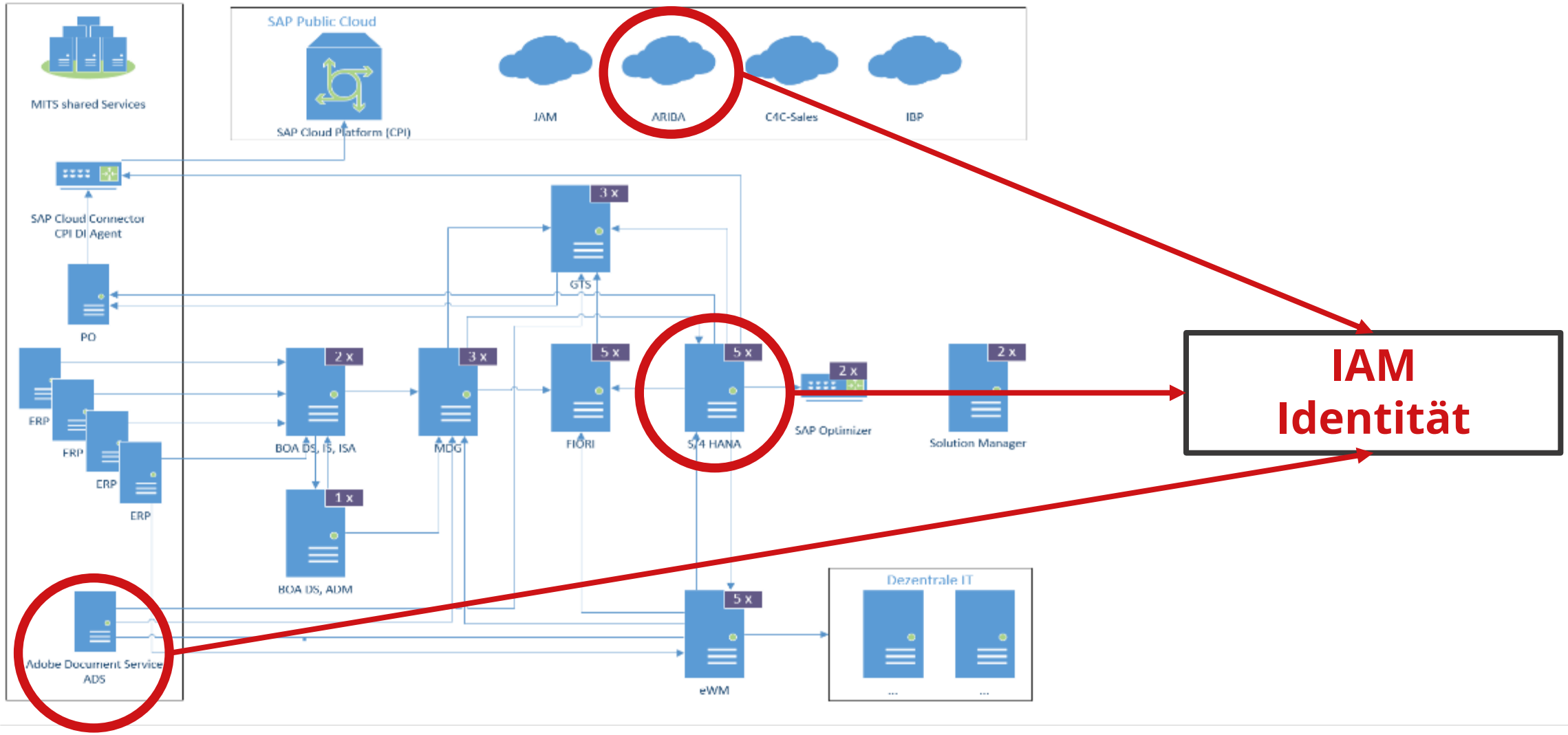
Xiting Security Platform (XSP)

- Zentrale Lösung zur Sicherstellung der Compliance in einer hybriden SAP-Landschaft
- Systemübergreifende Risikoanalysen
- Analyse-Dashboards zur Fehlererkennung und -behebung in der Landschaft
- Zentraler Hub zur Konsolidierung von Identitäten in der hybriden Landschaft
- Security Monitoring und Integration zu SIEM der gesamten Landschaft
- **Erweiterung der vorhandenen Funktionalität der XAMS** und Orchestrierung von Tools und Prozessen
- Die XSP ist das **zentrale Compliance-Cockpit** zur Überwachung der hybriden SAP-Landschaft im Rahmen der **Xiting Security Management Suite**

Die XSP als zentrale cloud-basierte Plattform für die Cloud (und On-Prem)

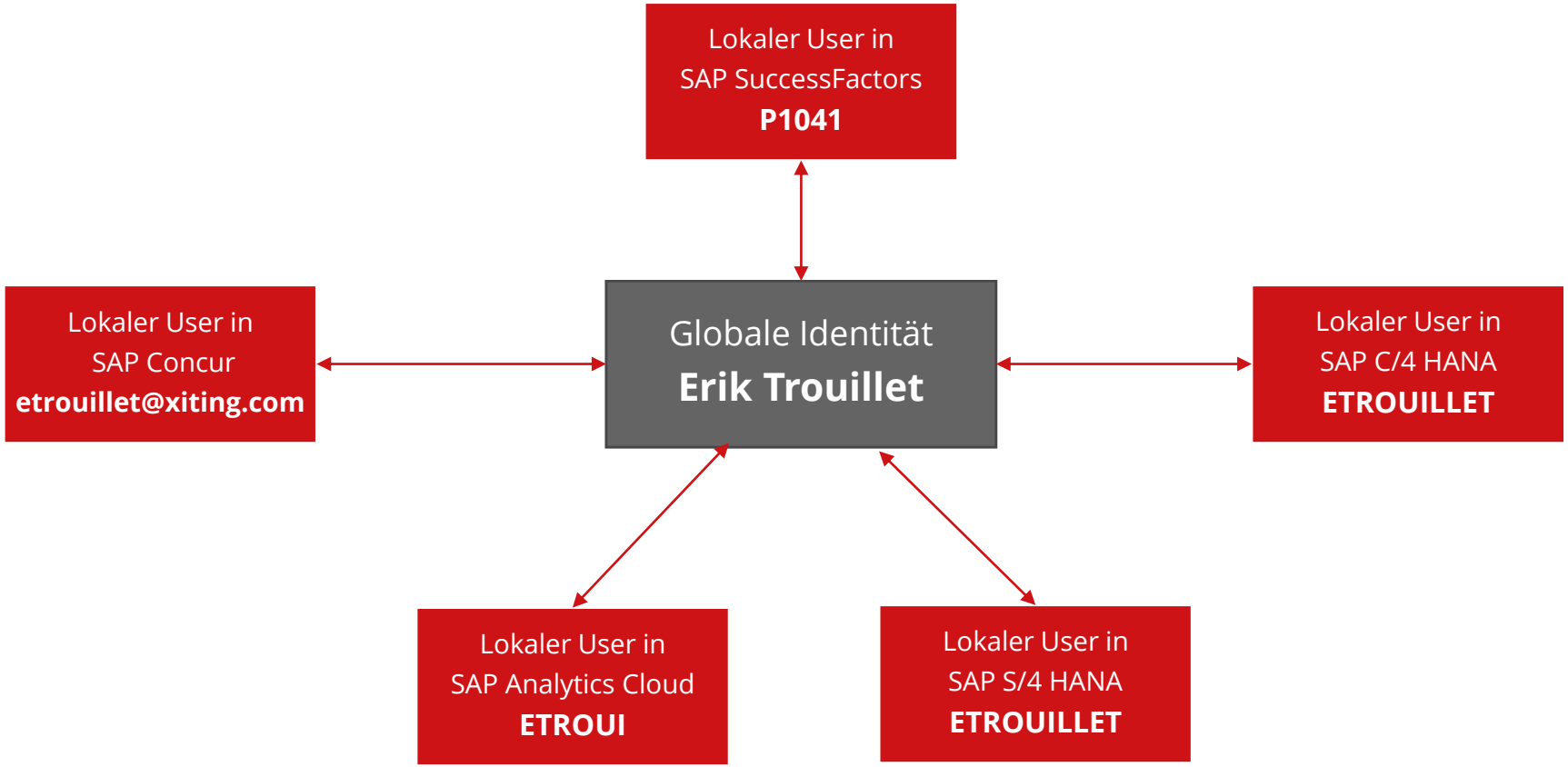


Identitäten in hybriden SAP Landschaften



Identity Consolidation

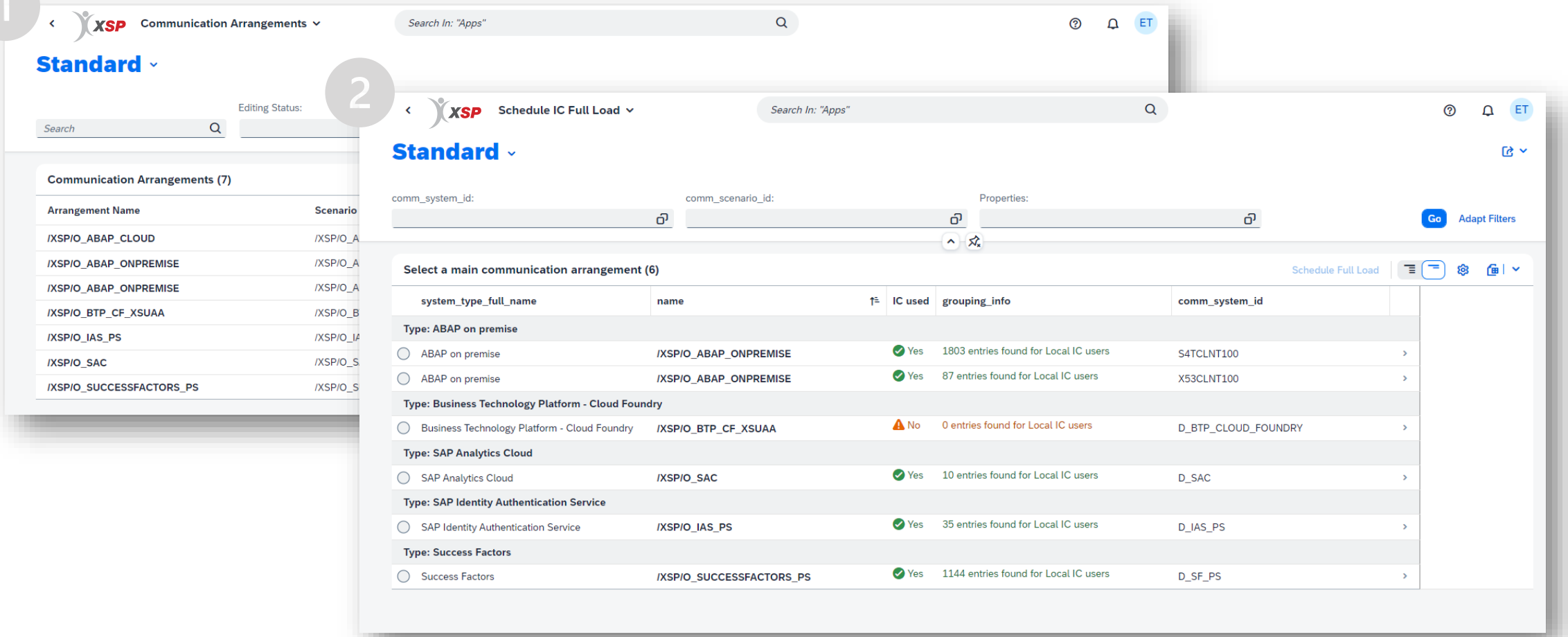
- Konsolidierung der lokalen Benutzer zu einer **globalen Identität**



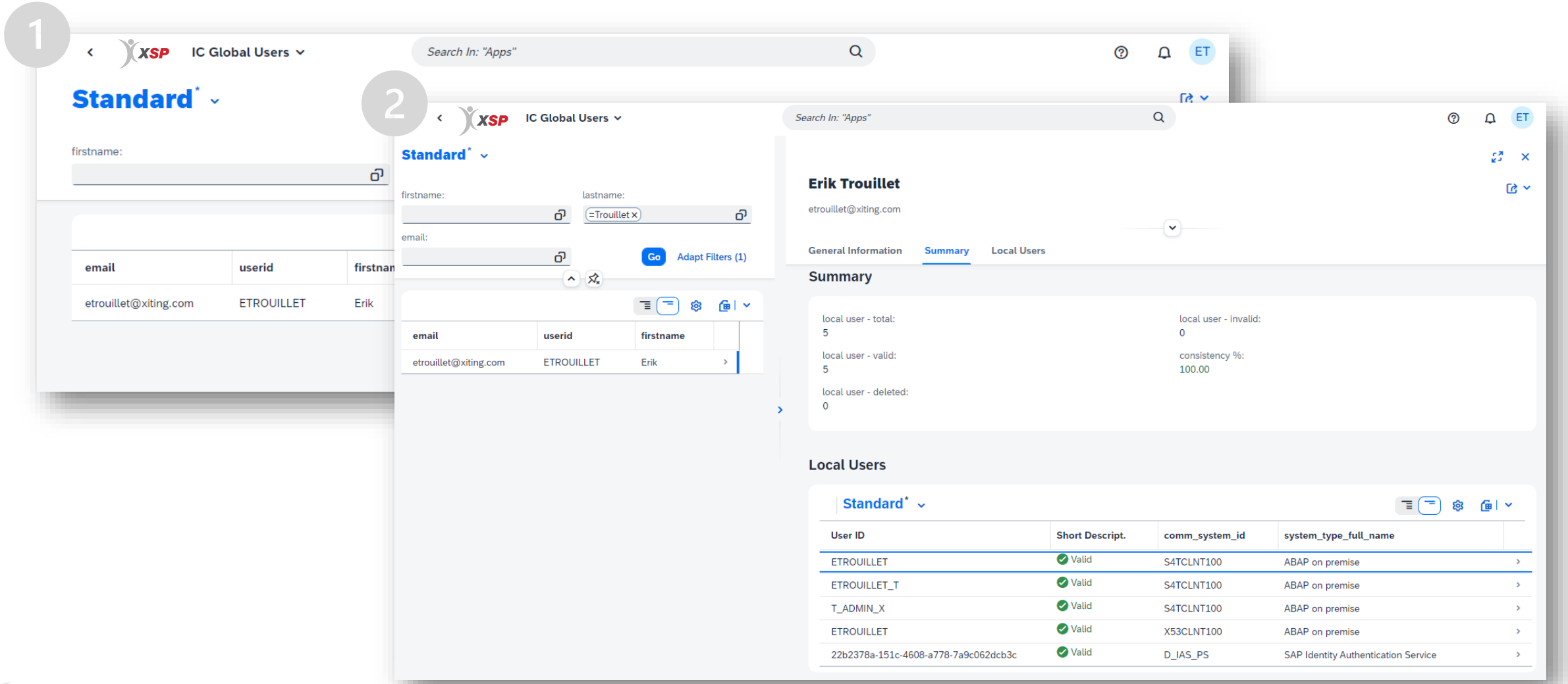
Schnelle Einrichtung der Identity Consolidation

1

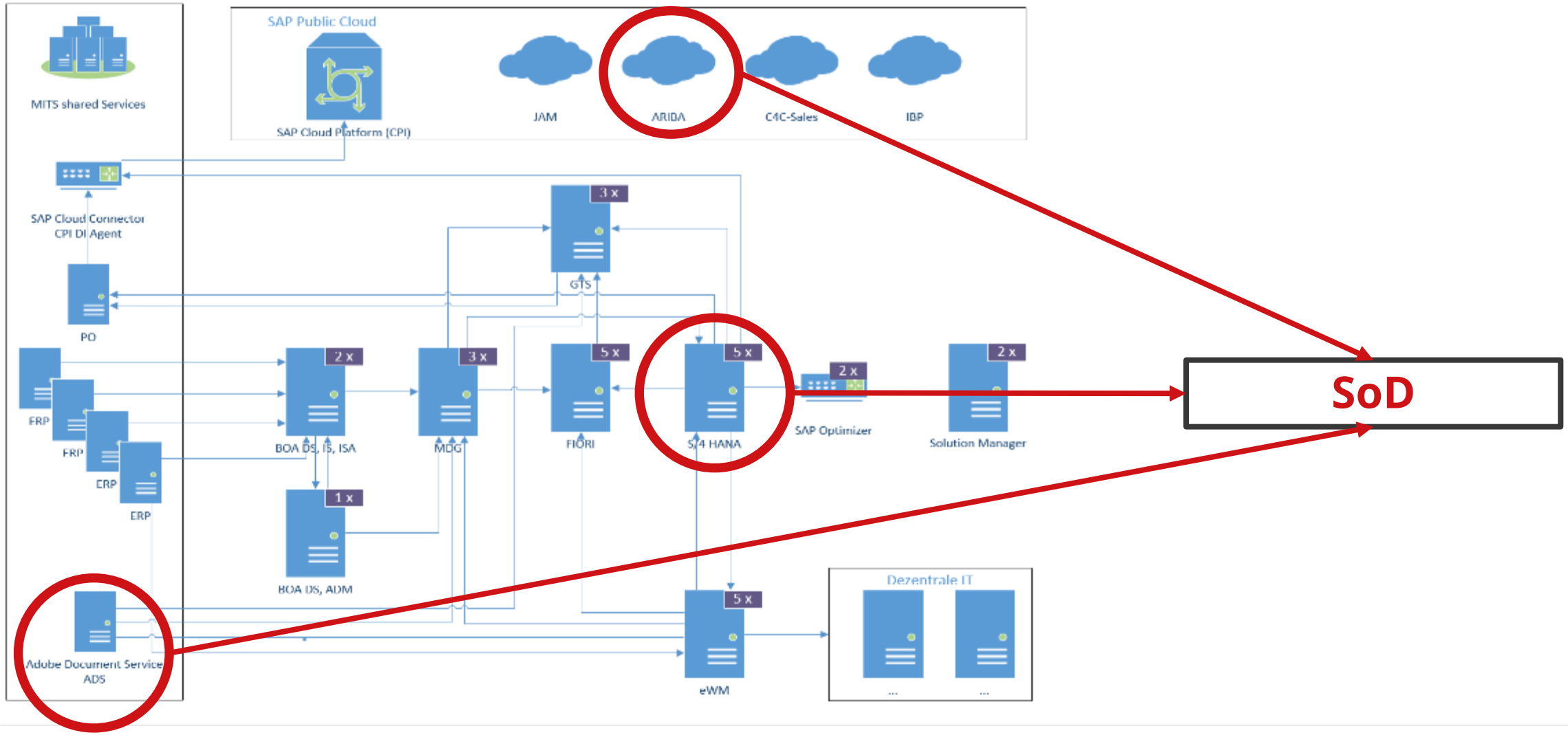
2



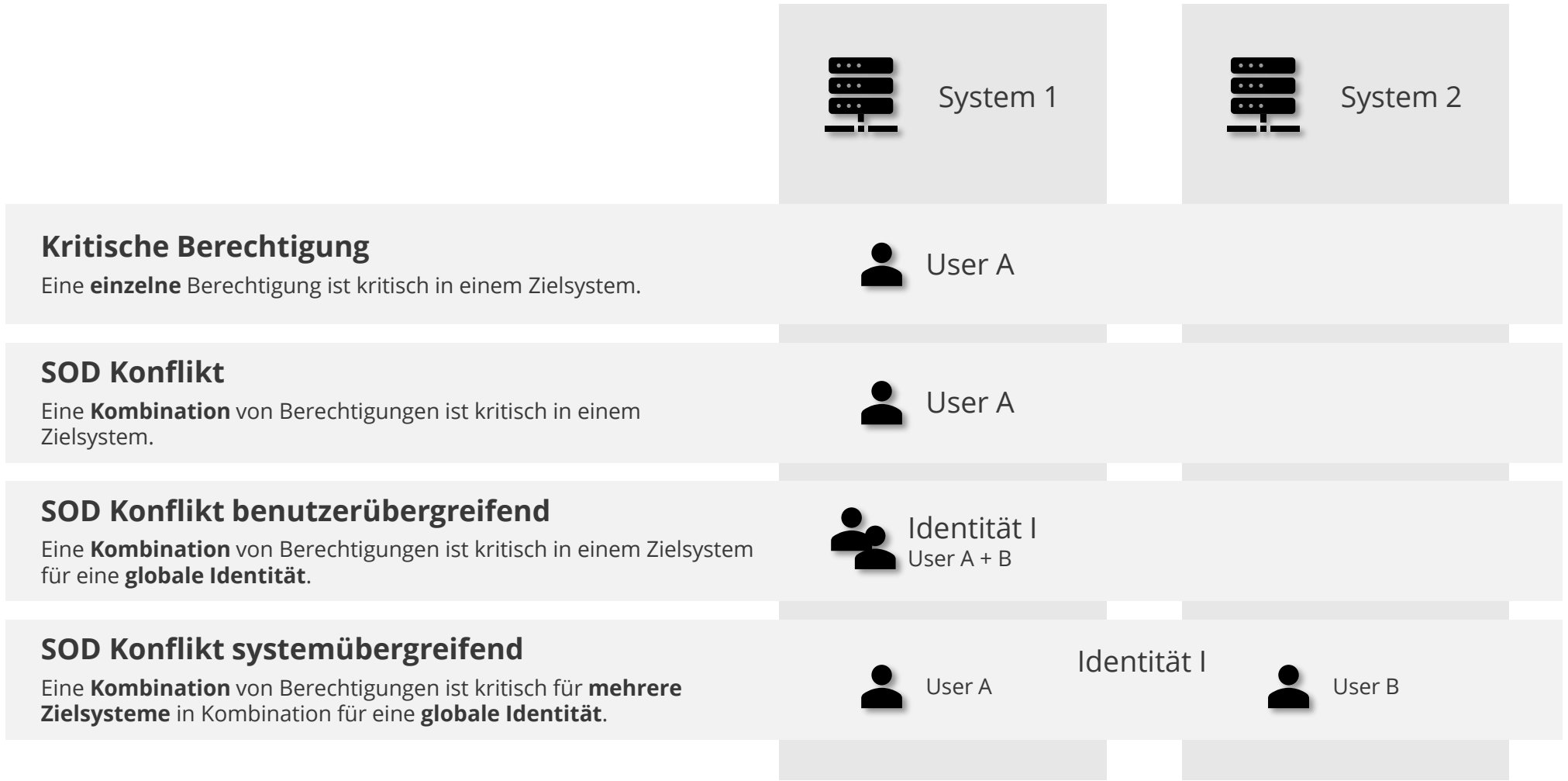
XSP: Eine globale Identität



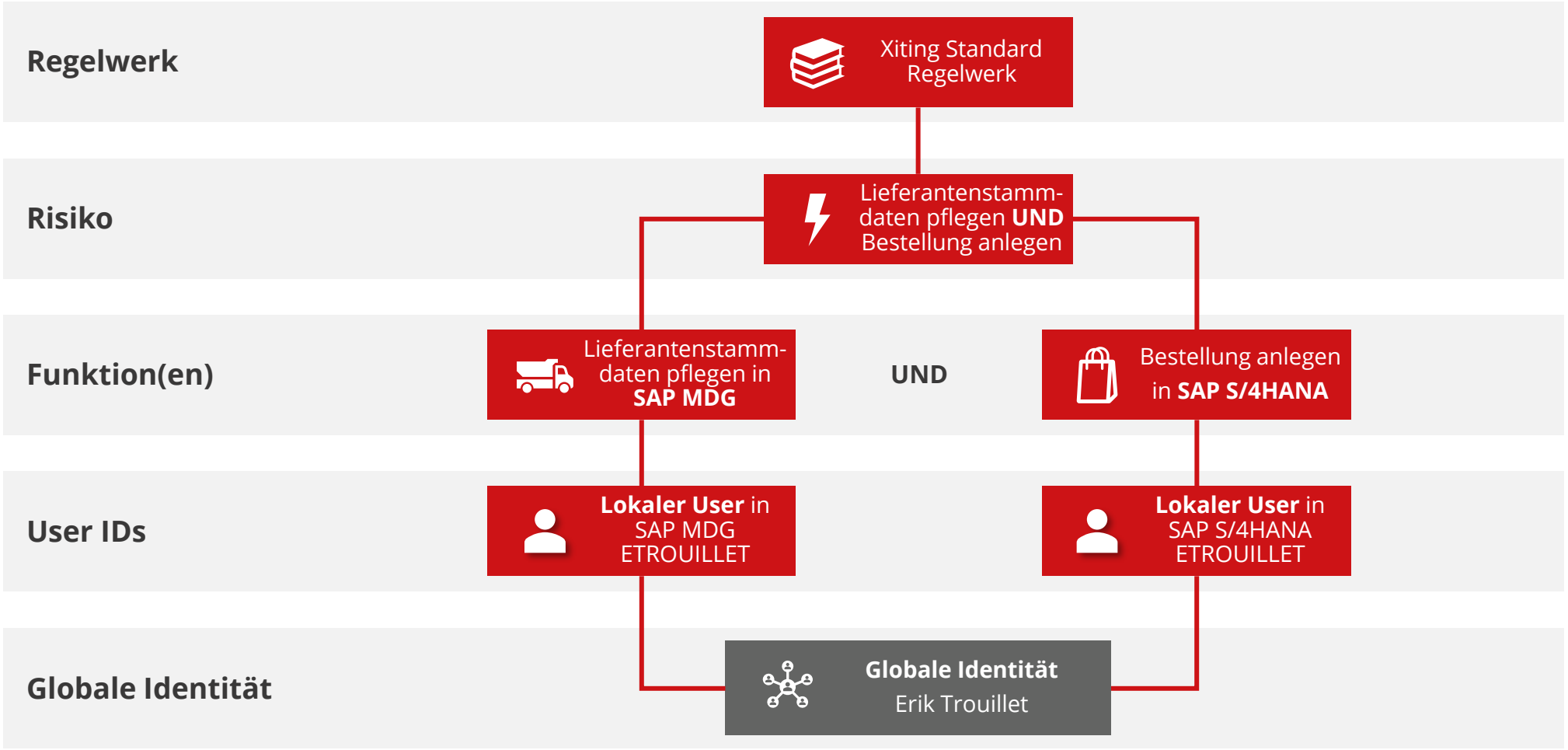
Systemübergreifende Risiken in hybriden SAP Landschaften



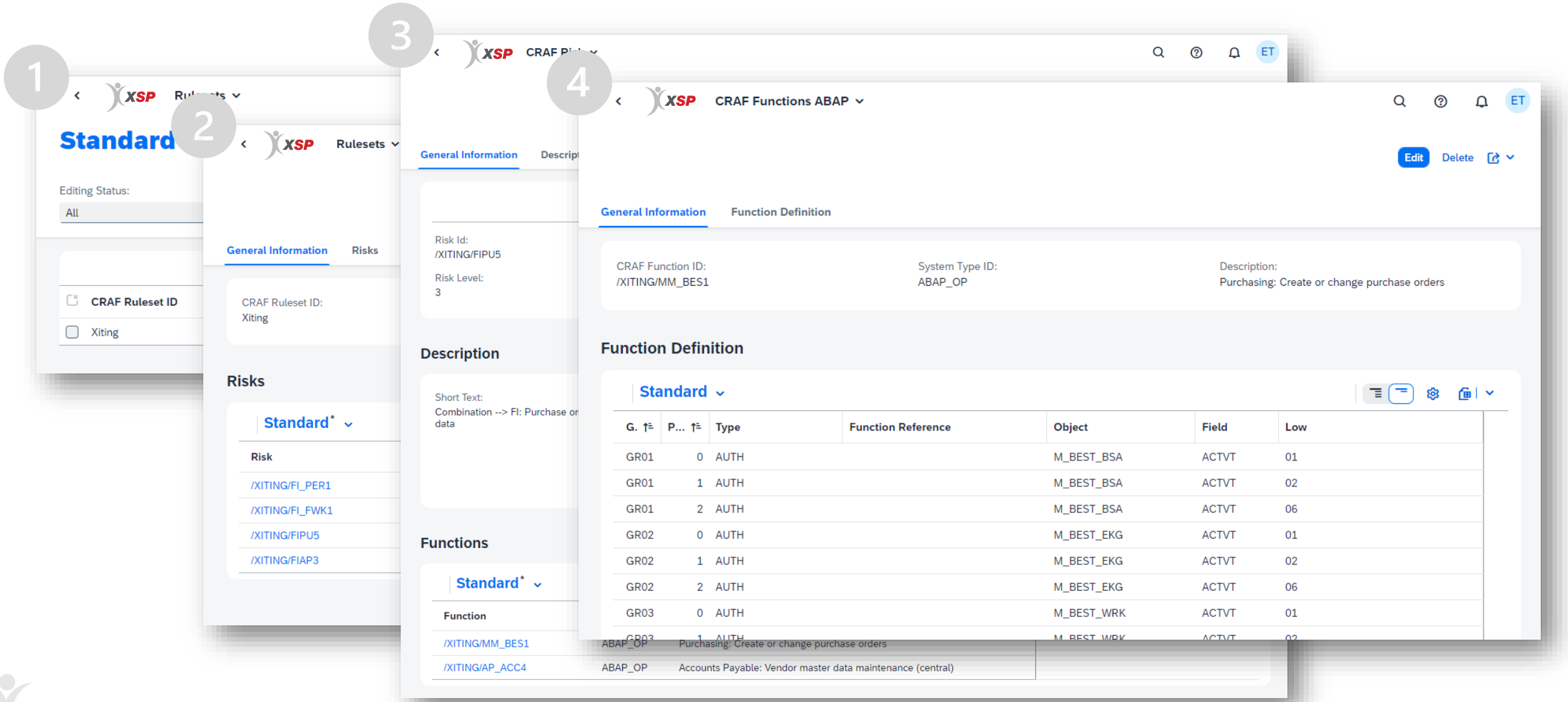
Die verschiedenen Risikoarten



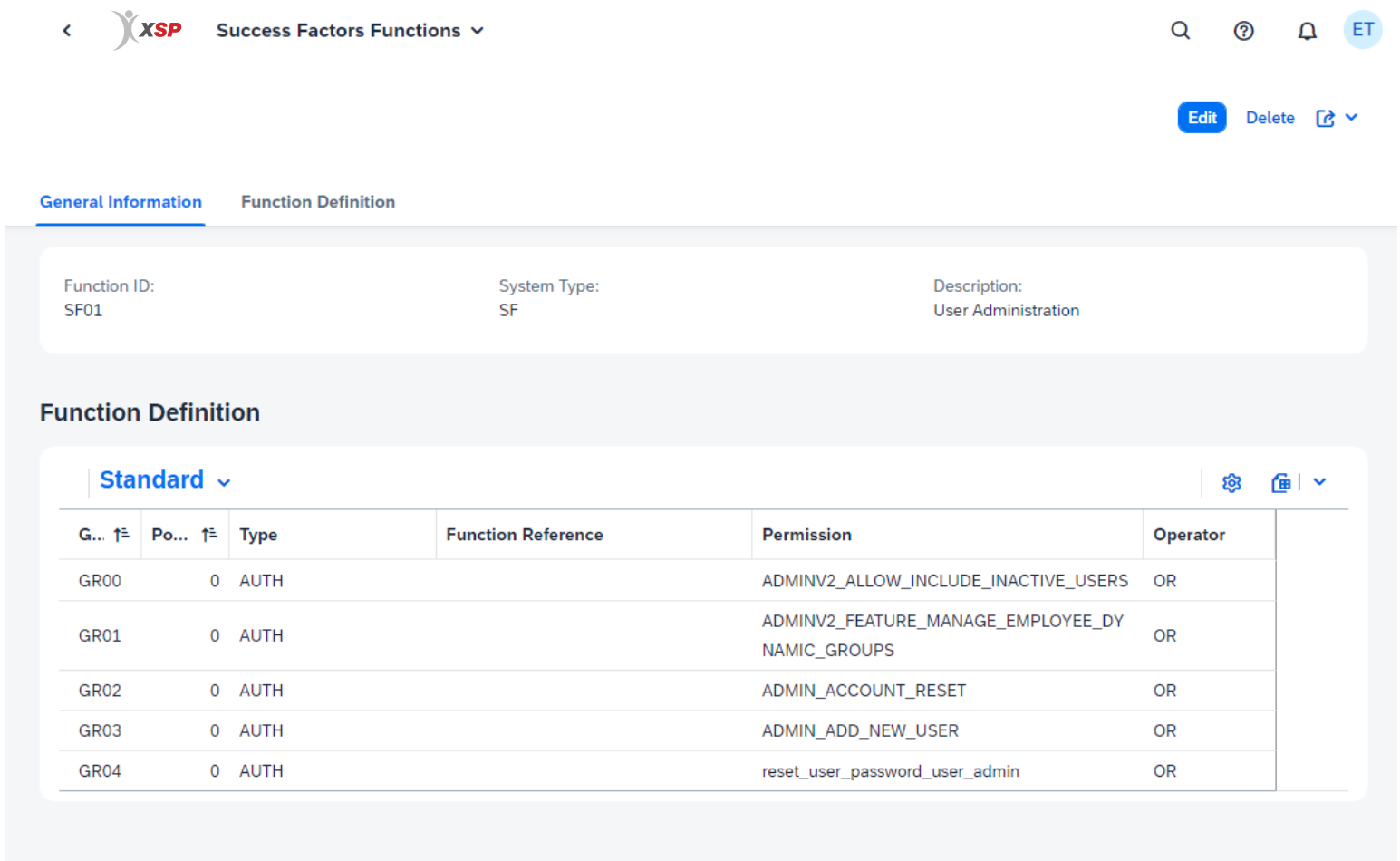
Systemübergreifende Risikoanalyse



XSP: Ein zentrales Regelwerk

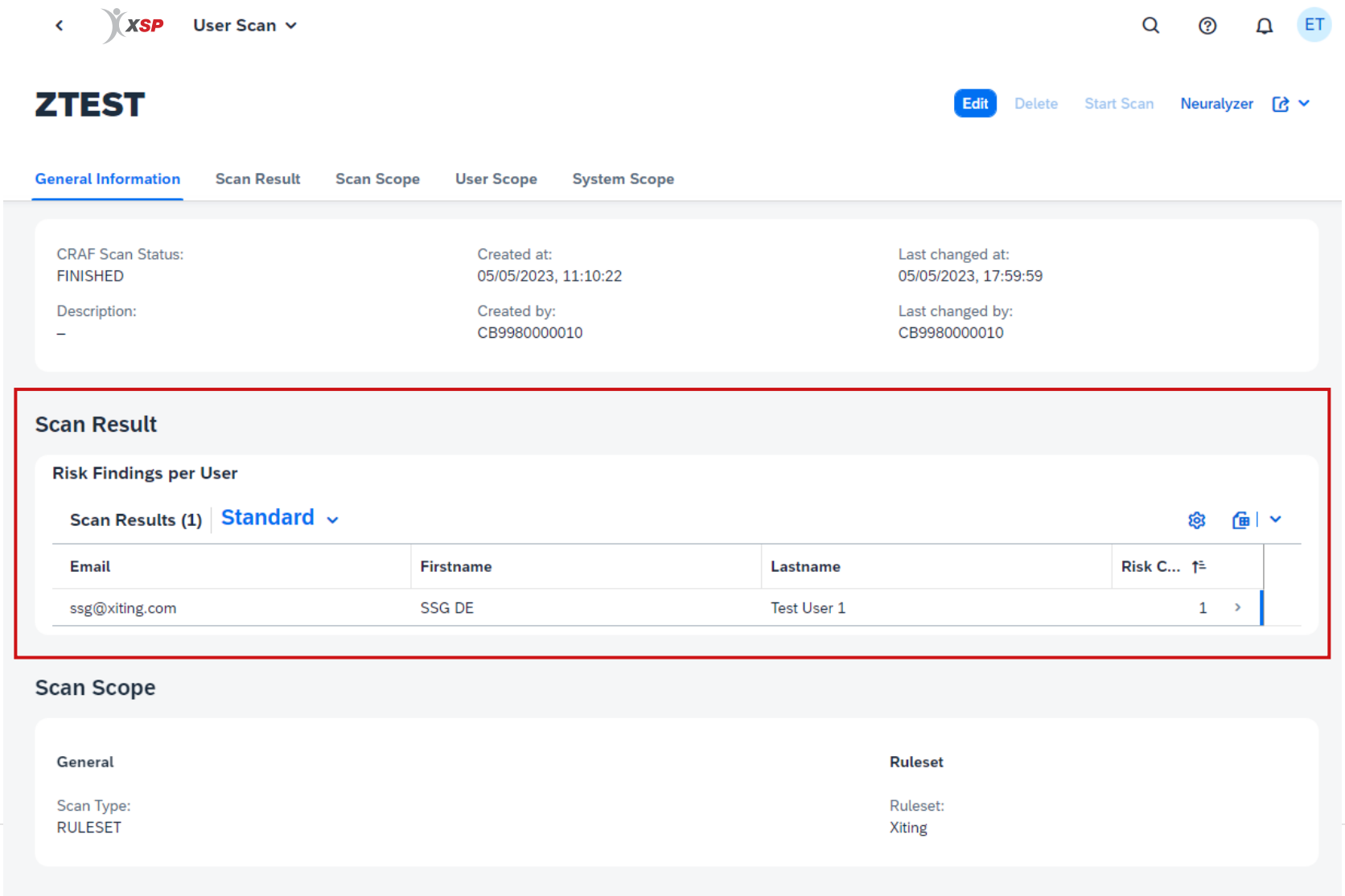


Unterstützung von anderen SAP und Non-SAP Lösungen



G...	Po...	Type	Function Reference	Permission	Operator
GR00	0	AUTH		ADMINV2_ALLOW_INCLUDE_INACTIVE_USERS	OR
GR01	0	AUTH		ADMINV2_FEATURE_MANAGE_EMPLOYEE_DYNAMIC_GROUPS	OR
GR02	0	AUTH		ADMIN_ACCOUNT_RESET	OR
GR03	0	AUTH		ADMIN_ADD_NEW_USER	OR
GR04	0	AUTH		reset_user_password_user_admin	OR

Benutzer Risikoanalyse



Resultate adhoc einsehbar sobald die Prüfung abgeschlossen wurde.

User Scope

General

Scan all users for selected systems:
No

Global Users

Standard*

User	Firstname	Lastname	UserId
ssg@xiting.com	SSG DE	Test User 1	SSG_DE_01

Globale Identität

System Scope

General

Scan all systems for selected users:
No

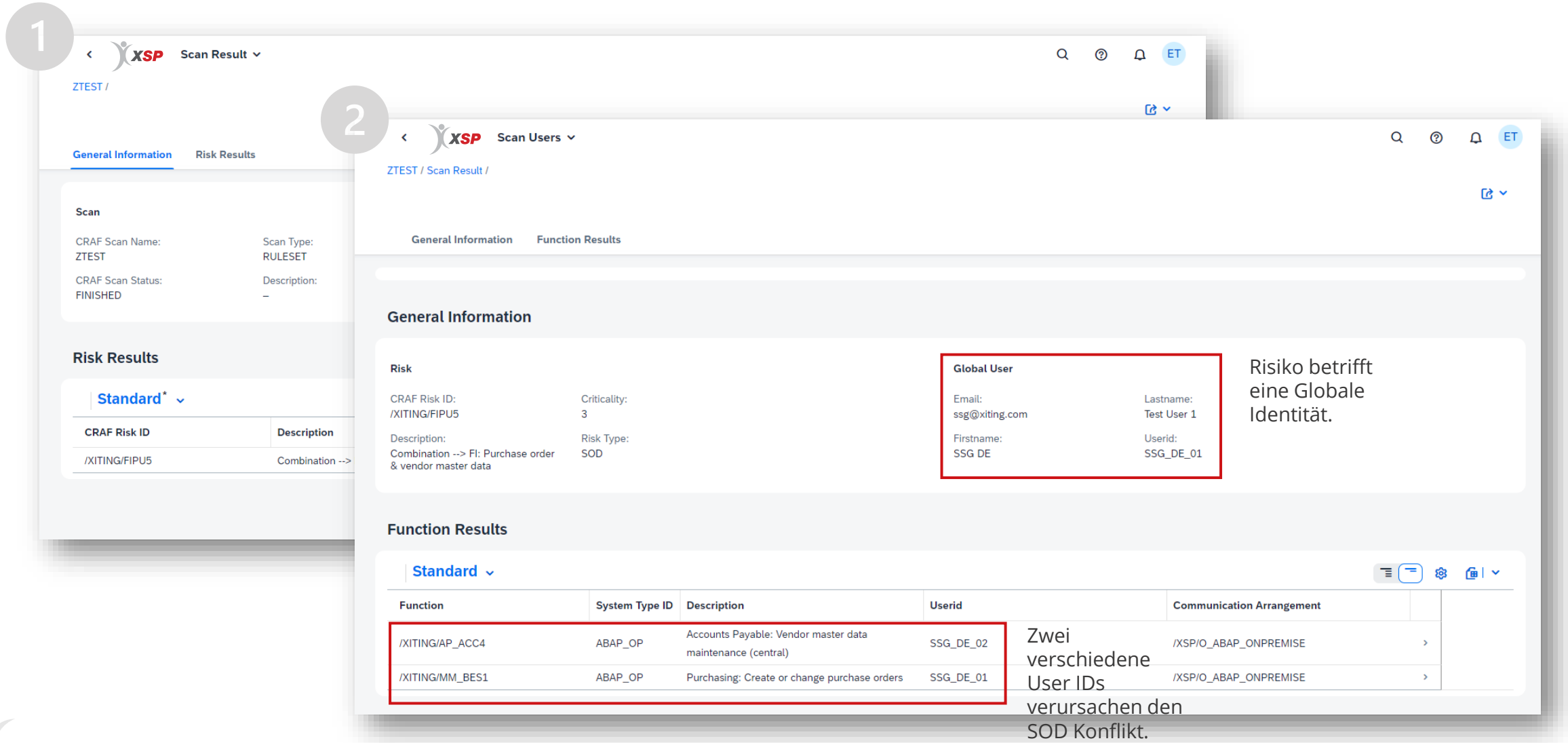
Communication Arrangements

Standard

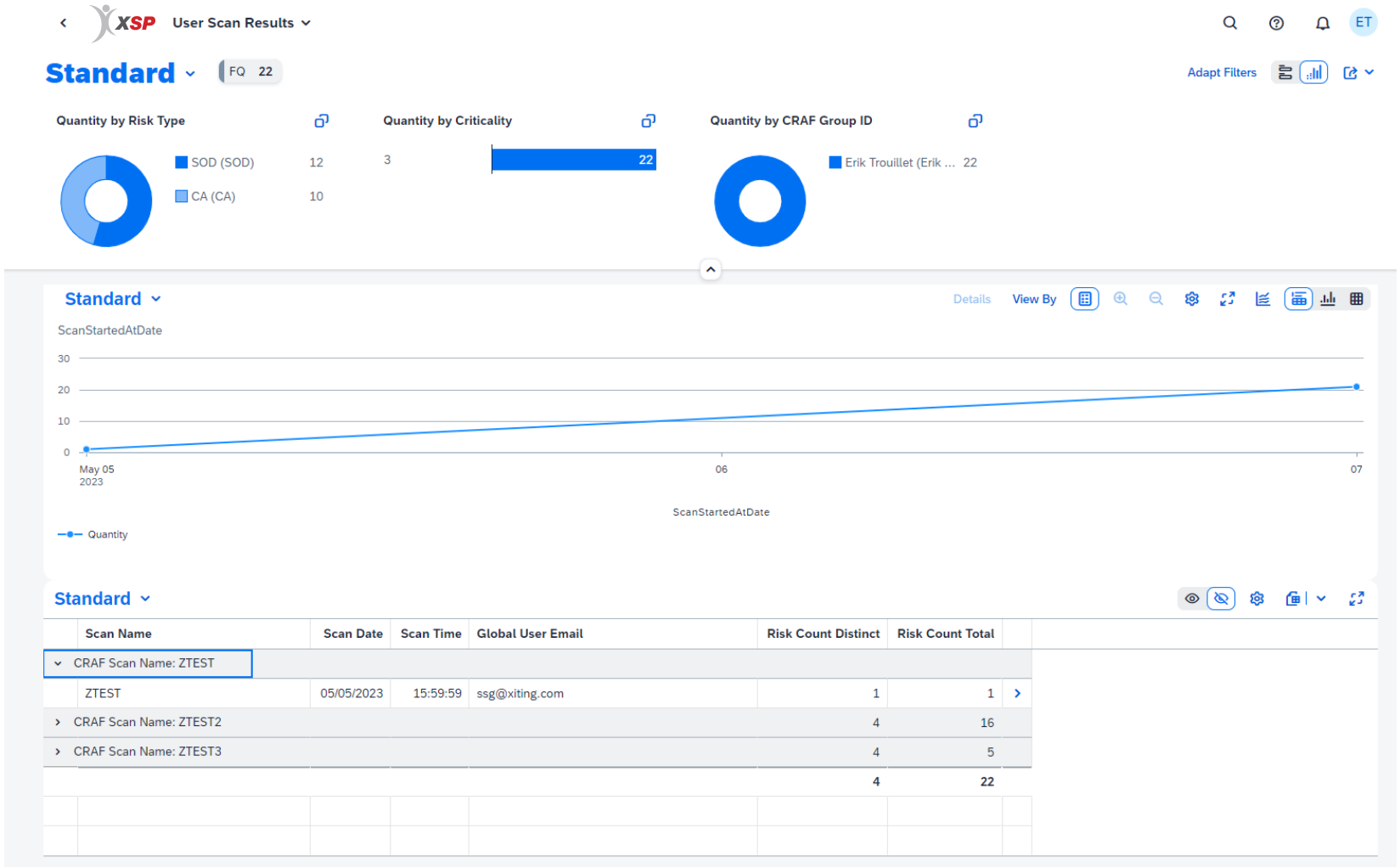
Communication Arrangement	System ID	Scenario ID
/XSP/O_ABAP_ONPREMISE	S4TCLNT100	/XSP/O_ABAP_ONPREMISE
/XSP/O_ABAP_ONPREMISE	X53CLNT100	/XSP/O_ABAP_ONPREMISE

System Scope

Benutzer Risikoanalyse: Resultate

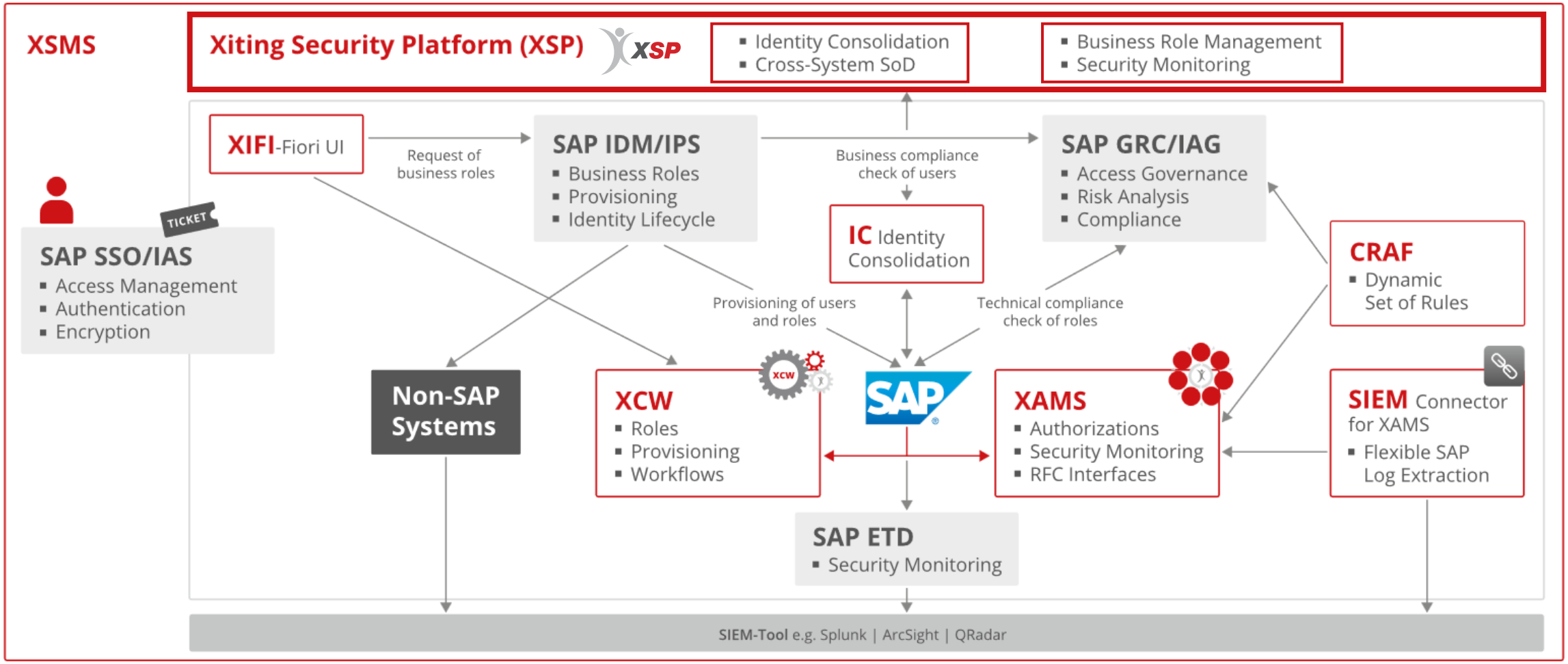


Benutzer Risikoanalyse: Neue Auswertungsmöglichkeiten

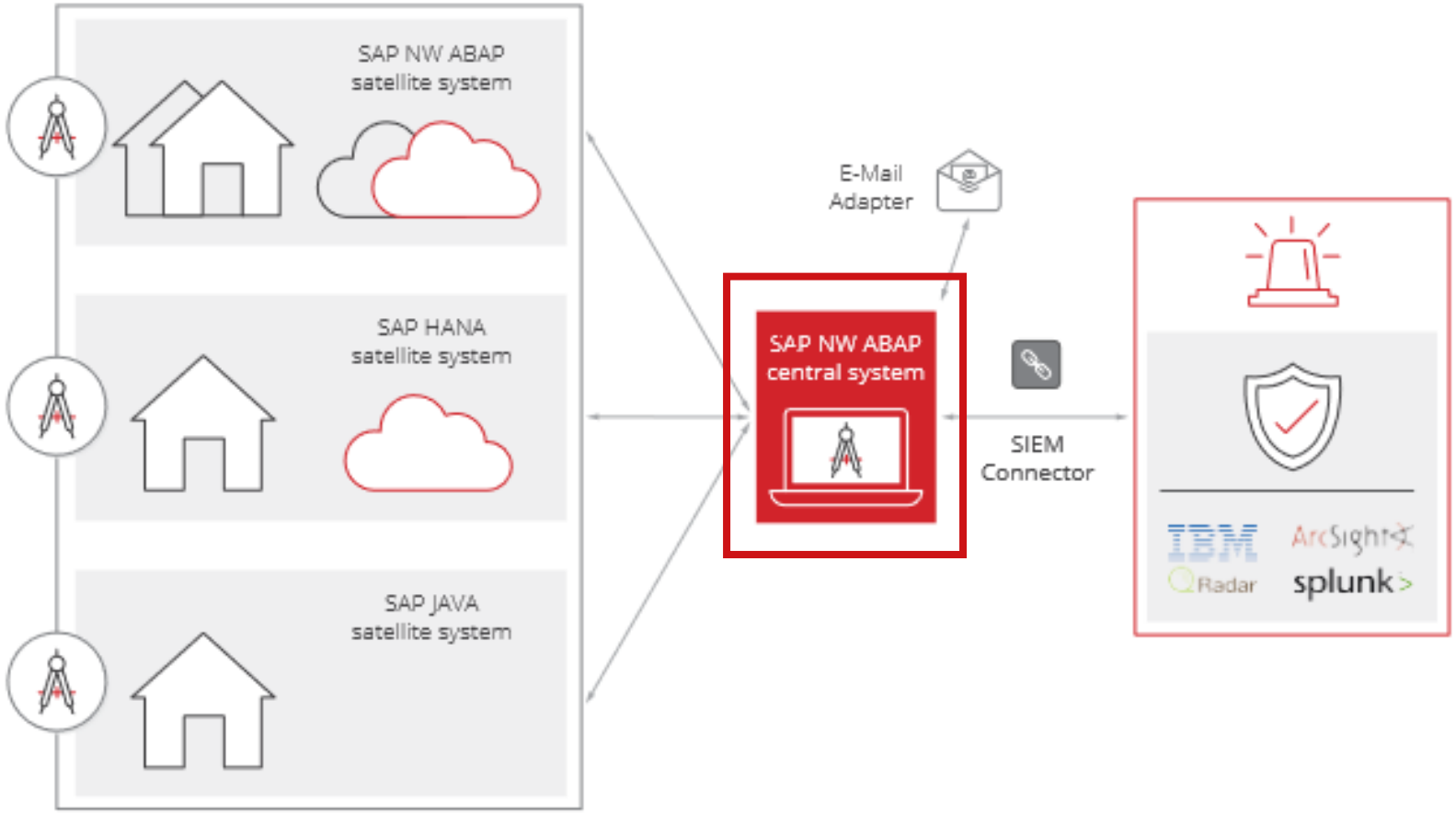


DEMO

Governance, Risk, Compliance und Security aus einer Hand



Bereitstellung der Daten für ABAP Systeme mit dem XAMS Security Architect



Erfüllung der GRC Anforderungen mit der XSP

- Die XSP wird von Grund auf als GRC-Tool entwickelt und soll sämtliche Anforderungen nativ erfüllen. Es werden die Stärken der XAMS genutzt um vor allem in den Bereichen Sicherheit und Skalierbarkeit profitieren zu können.


Governance-Unterstützung


Risikomanagement


Compliance-Management


Reporting- und Analysefähigkeiten


Benutzer-freundlichkeit


Integration


Sicherheit


Skalierbarkeit

Kapitel 4

Roadmap: Ein Ausblick

XSP Roll-out Plan

01

XSP Framework

Vision, Ziele, Planung
Grobkonzept,
Entscheid Technologie,
Integration, Infrastruktur

02

POC (intern)

Entwicklung Communication Framework, Identity Consolidation, Risk Analysis

03

POC (Pilotkunden)

Testphase und
Weiterentwicklung XSP

04

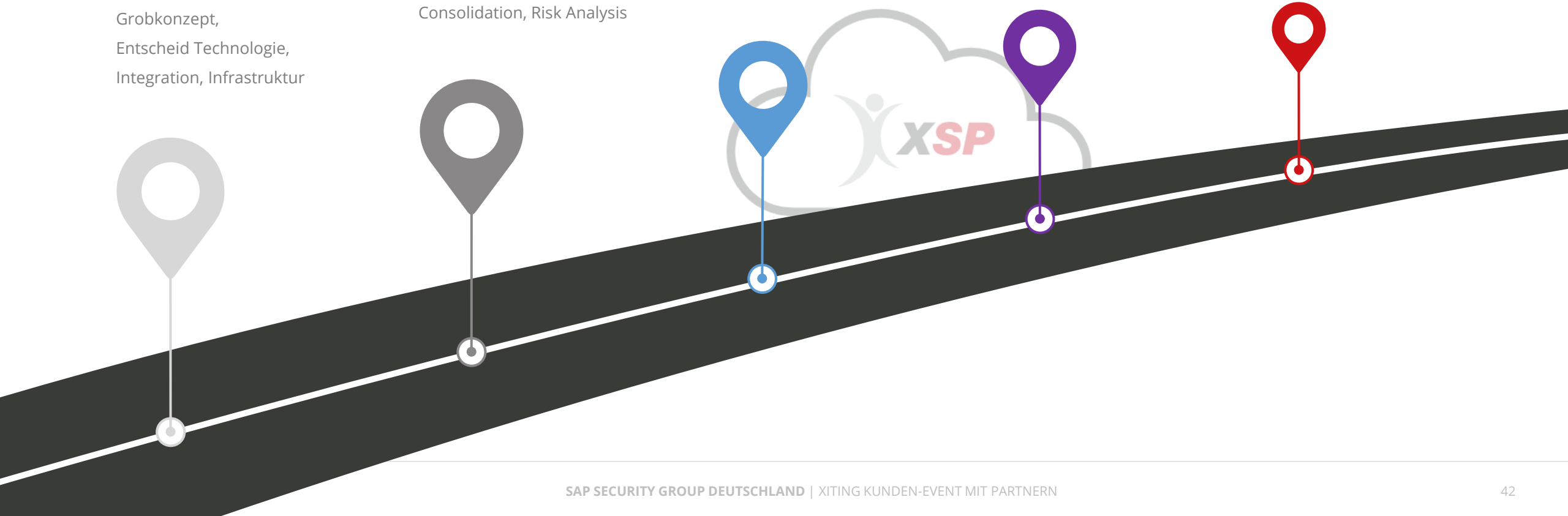
Main Release

Verfügbarkeit der XSP für
Bestands- und Neukunden

05

Feature Packs

Erweiterung der XSP mit
kurzen Releasezyklen



Use Cases in Planung

Identity & Access Governance

- Identity Consolidation
- Systemübergreifende Risiken
- Auswertungen, Bereinigung und Mitigation
- Role Mining und Business Rollen
- Notfallbenutzermanagement
- Security Audits

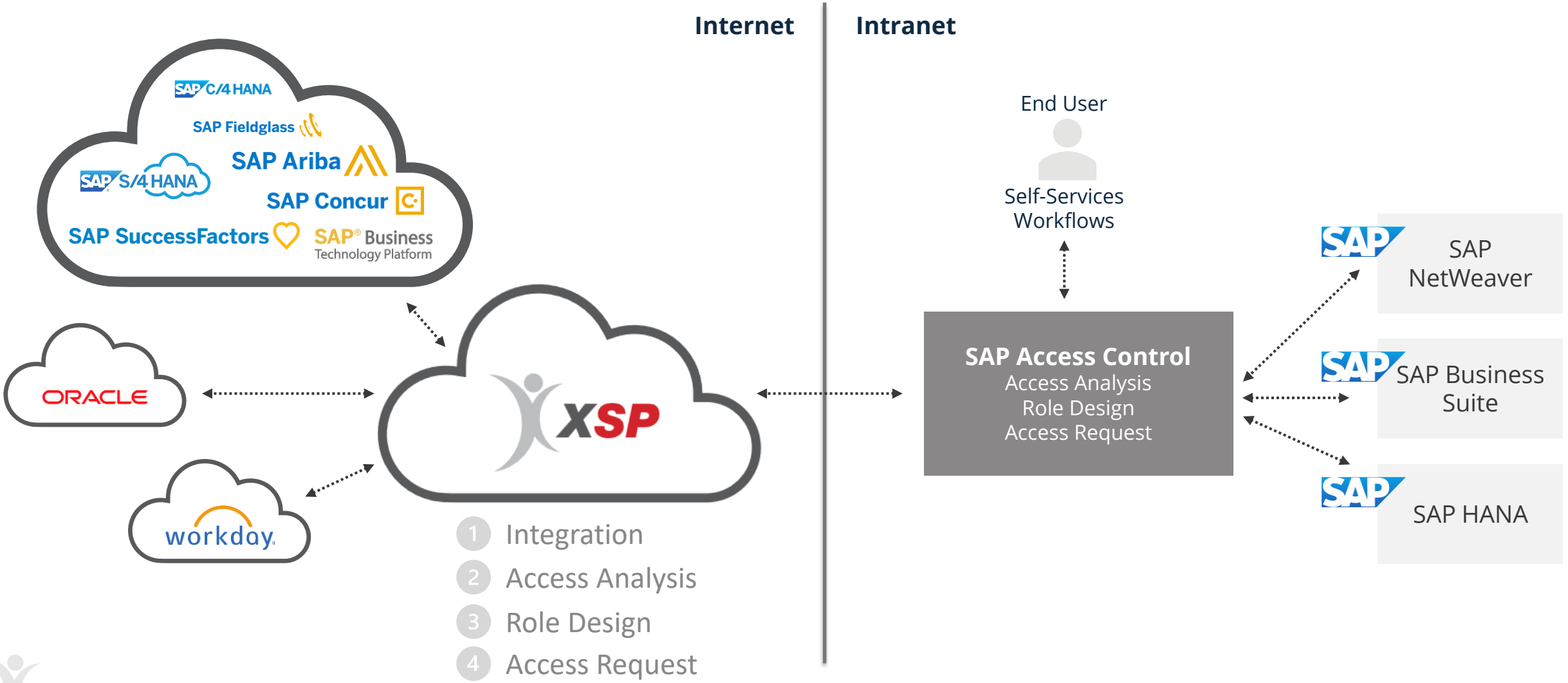
Security Monitoring & Threat Detection

- Zentrales Security Monitoring für sämtliche SAP Applikationen
- Echtzeit Alarmierung
- SIEM Integration
- Erkennung von Bedrohungen und Betrug
- SOAR

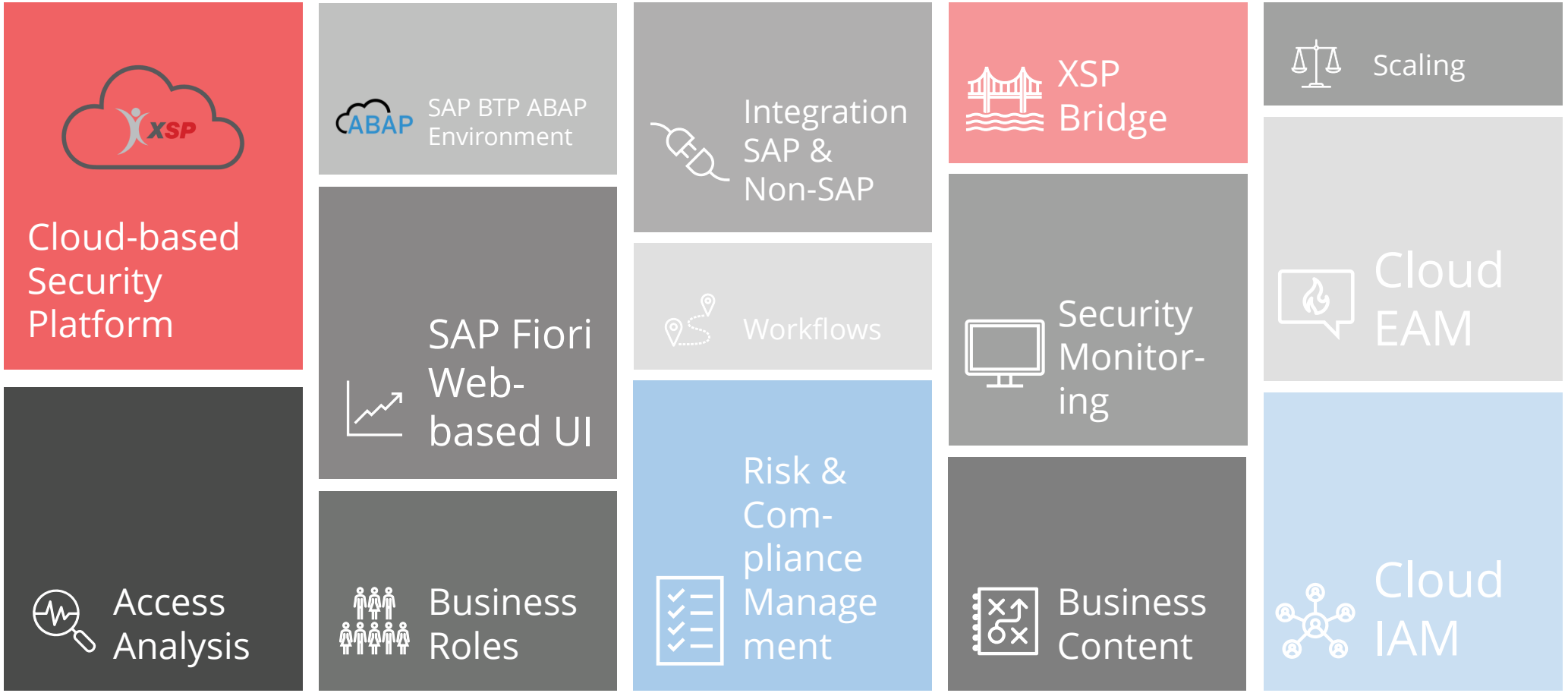
Workflows

- Regelkonforme Provisionierung von Berechtigungen
- Simulation SOD / Kritische Berechtigungen als Teil von Workflows
- Benutzer-Rezertifizierung

XSP Bridge


Internet
Intranet
SAP C/4 HANA
SAP Fieldglass
SAP Ariba
SAP S/4 HANA
SAP Concur
SAP SuccessFactors
SAP Business Technology Platform
ORACLE
workday
XSP
End User
Self-Services Workflows
SAP Access Control
Access Analysis
Role Design
Access Request
SAP NetWeaver
SAP Business Suite
SAP HANA
1 Integration
2 Access Analysis
3 Role Design
4 Access Request

XSP im Überblick



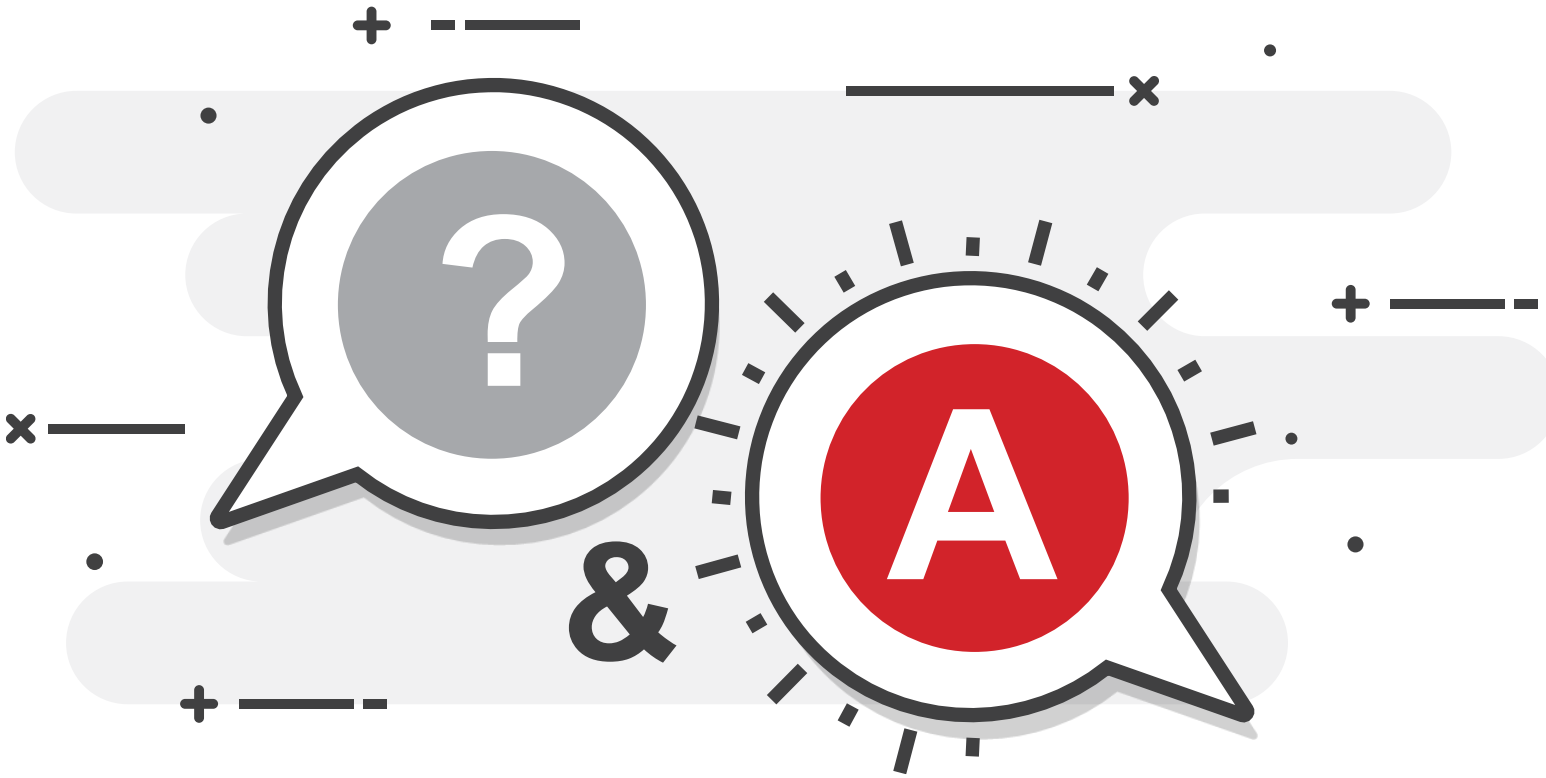
Xiting Security Platform – Schauen Sie mal vorbei

SCAN ME

Revolutionieren Sie Ihr SAP Security Management mit der Xiting Security Platform (XSP)

XSP

Fragen und Diskussionen



Fragen und Diskussionen

Erik Trouillet

Managing SAP

Security Consultant

Olaf Sauer

Leiter Direct Sales

Dankeschön

Für Ihre Aufmerksamkeit

Wenn Sie weitere Informationen benötigen, können Sie uns gern kontaktieren.