SAP Security Group Deutschland

Xiting Kunden-Event
mit Partnern

9./10.
MAI
2023

Workshop
„Strategische Absicherung in SAP Security Projekten“

Adrian Bayer-Szegedi | Q_Perior

Güterbahnhof Heidelberg

Agenda

1. Strategic Alignment Model
2. Change by Organization
3. Change by Technology
4. Golden Circle

Kapitel 1

Strategic Alignment Model

Wir wollen Ihre SAP Security Projekte strategisch absichern

Q_PERIOR

2 „Change by Technology“

Strategic Alignment Model

Ihr Business

Technologie

1 „Change by Organization“

Strategisch

Ihr operativer Betrieb

Business-Strategie

- Alleinstellungs-merkmale & Vorteile
- Geschäftsmodell & Marktumfeld
- Unternehmens-Kooperationen

IMS | SAFe | Scrum ban | CCoE

Fachbereich

- Hierarchische bzw. agile Organisation & Skillset
- Geschäftsprozesse & Arbeitsmodelle

IT Strategie

- IT-Services & Architektur
- IT-Organisation & Skill-Set
- IT-Kooperationen

XITING quality | ibs Schreiber | SAP S/4 HANA | paricon | u.v.m...

IT Services

- Hierarchische bzw. agile Organisation & zentrale bzw. dezentrale Governance
- DevSecOps
- IT-System & Platform

IMS = Integriertes Mgmt. System
SAFe = Scaled Agile Framework
CCoE = Competence Center of Excellence

Q_PERIOR bietet Ihnen SAP, Security & Technologien aus einer Hand an

SAP

SAP Program- & Project Management

SAP Finanzen & Controlling

SAP Supply Chain Management

SAP Business Intelligence & Analytics

SAP Technologie & Innovation

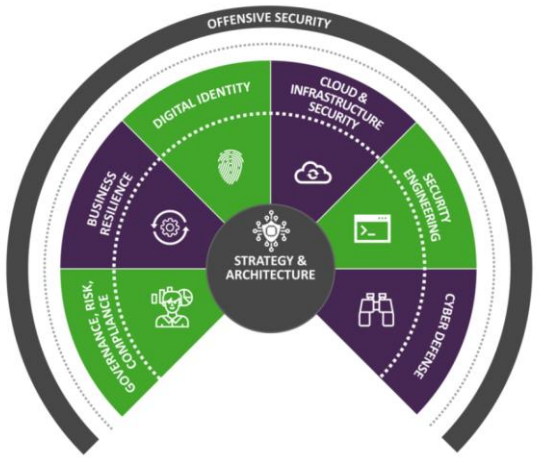
SAP Customer Experience

Security

SAP Security Assessments & Transformation

SAP Security Application Lifecycle Management

Cybersecurity Dienstleistungen



Governance Risk Compliance & Business Resilience

Digital Identity & Security Engineering

Cyber Defense, Cloud & Infrastructure Security

Technologien

SAP Gold Partner

ITing quality

ibs Schreiber

paricon

u.v.m...

Kapitel 2

Change by Organization

Ihr Business entscheidet über die passende Technologie

Strategic Alignment Model

Ihr Business

Technologie

Strategisch

Ihr operativer Betrieb

1 „Change by Organization“

Business-Strategie

IT Strategie

Fachbereich

IT Services

Management-Systeme basieren auf verschiedenen gesetzlichen Grundlagen

1. Compliance Management System (CMS)

Basis: IDW PS 980

Wesentliche Zwecke:

- Schaffung und Erhaltung einer nachhaltigen Compliance-Kultur
- Frühzeitige Erkennung wesentlicher Risiken bei Regelverstößen
- Maßnahmenentwicklung, um Regelverstöße zu verhindern
- Implementierung eines Reaktionsmechanismus bei Regelverstößen

2. Informations-Management System (ISMS)

Basis: ISO 2700x / BSI IT-Grundschutz

Wesentliche Zwecke:

- Definition von Verfahren und Regeln zur Informationssicherheit
- Steuerung und Kontrolle möglicher Informationssicherheitsrisiken
- Maßnahmenentwicklung, um Risiken zu minimieren und Schutzbedarfe aufrechtzuerhalten
- Fortlaufender Verbesserungsprozess

3. Datenschutz Management System (DSMS)

Basis: Datenschutz-Grundverordnung

Wesentliche Zwecke:

- Planung, Organisation, Steuerung und Kontrolle der datenschutzrechtlichen Vorgaben
- Integration in die Gesamtorganisation
- Prozessentwicklung, um Betroffenenrechte gerecht zu werden
- Maßnahmenentwicklung, um datenschutzrechtliche Risiken und Vorfälle zu vermeiden

4. Business Continuity Management System (BCMS)

Basis: ISO 22301

Wesentliche Zwecke:

- Implementierung eines Prozesses, um schädliche Vorfälle zu vermeiden
- Frühzeitige Erkennung möglicher Risiken und Gefahren
- Kontinuierliche Dokumentation der Prozesse und Vorkommnisse innerhalb eines Management Systems
- Maßnahmenentwicklung zur Verhinderung oder schnellen Erholung von Vorfällen

Die Systeme können zum Integrierten Management System umstrukturiert werden

Säulen	1. CMS	2. ISMS	3. DSMS	4.BCMS
Compliance	✓	✓	✓	✓
Strategie & Governance	✓	✓	✓	✓
Risiko Management	✓	✓	✓	✓
Richtlinien & Kontrollen	✓	✓	✓	✓
Kultur & Kommunikation	✓	✓	✓	✓
Überwachung & Reporting	✓	✓	✓	✓
Kontinuierliche Verbesserung	✓	✓	✓	✓
Incident-Management	✓	✓	✓	✓
Audit	✓	✓	✓	✓

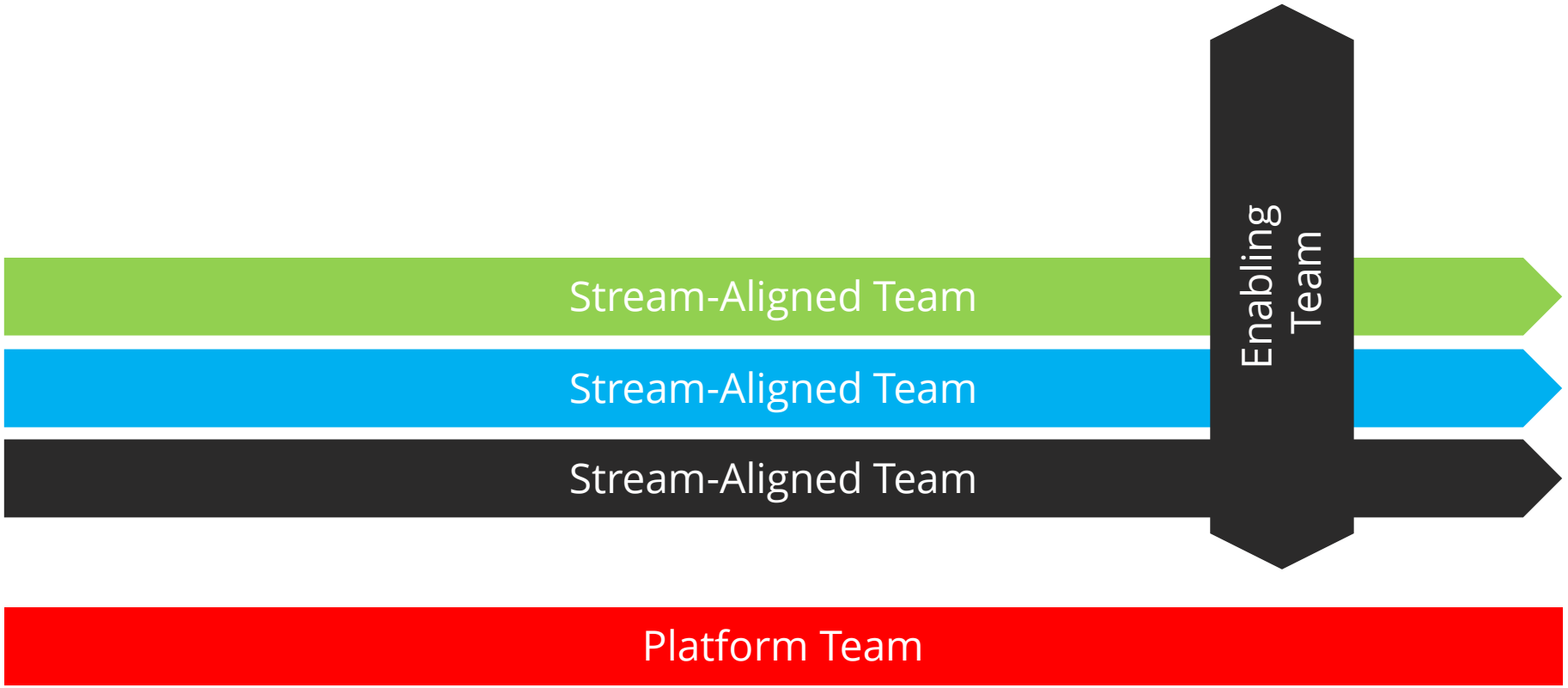
Synergien der Management-Disziplinen:

- Alle Management Systeme bauen auf neun übereinstimmenden Säulen auf
- Diese bilden die Basis bei der Implementierung eines jeden Management-Systems
- Auf der nächsten Prozessebene erfolgt dann die Detailierung hinsichtlich des besonderen Themenbereichs
- Die Grundsätzlichen Prozesssäulen sind gleich

Fazit:

- Ein integriertes Management-System schafft Synergien und hebt Effizienzen im Unternehmen

Das Enabling Team kann das Stream-Aligned Team unterstützen

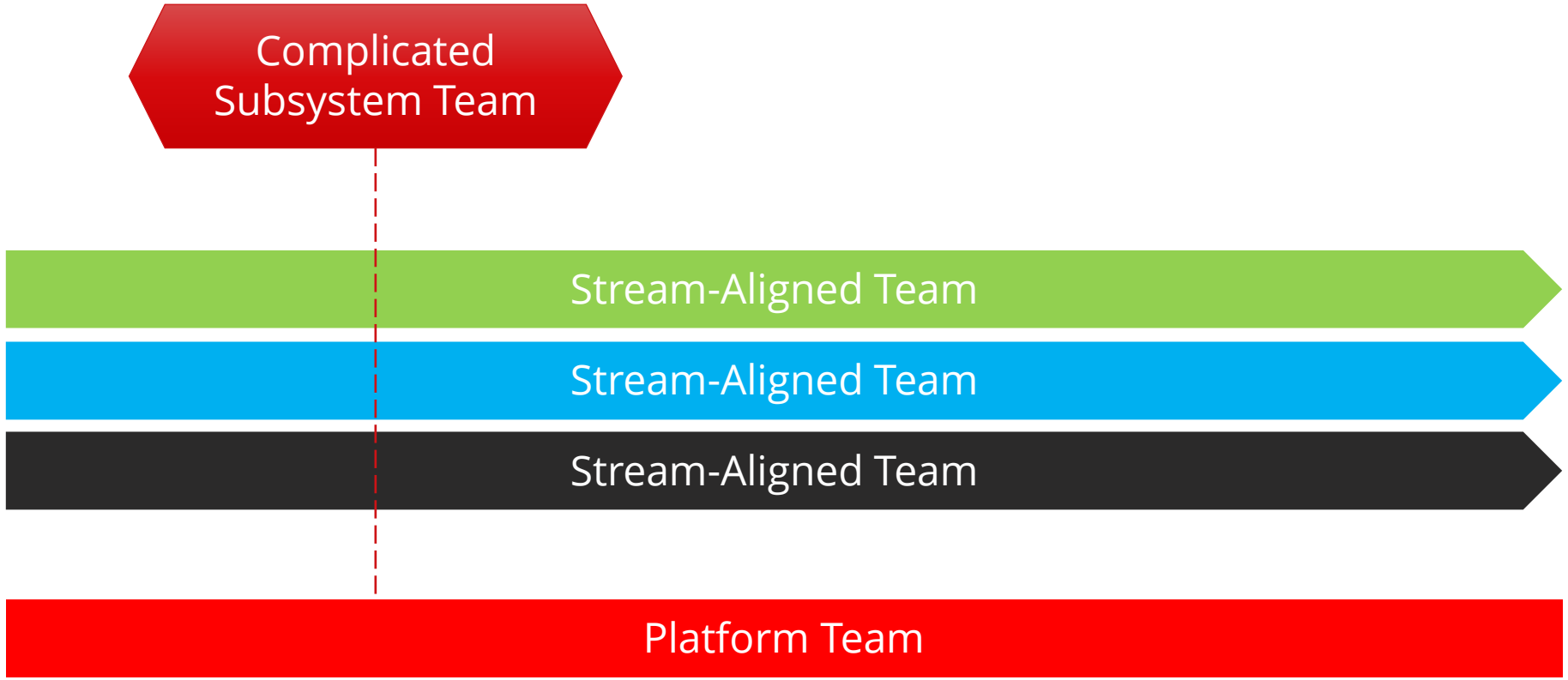


Das Enabling Team muss rechtzeitig via KANBAN angefordert werden

Stream-Aligned Team	Enabling Team
Sprint N	SPRINT N+/-x

Stream-Aligned Team	Enabling Team
SCRUM	KANBAN

Das Complicated-Subsystem Team vereinfacht die Technologie Platform



Das Complicated-Subsystem Team entwickelt mit dem Platform Team

Platform Team

Sprint N-x

Complicated-Subsystem Team

SPRINT N-x

Platform Team

SCRUM/ KANBAN

Complicated-Subsystem Team

SCRUM/ KANBAN

Kapitel 3

Change by Technology

Die passende Technologie entscheidet über Ihr Business

2 „Change by Technology“

Strategic Alignment Model

Ihr Business

Technologie

Strategisch

Ihr operativer Betrieb

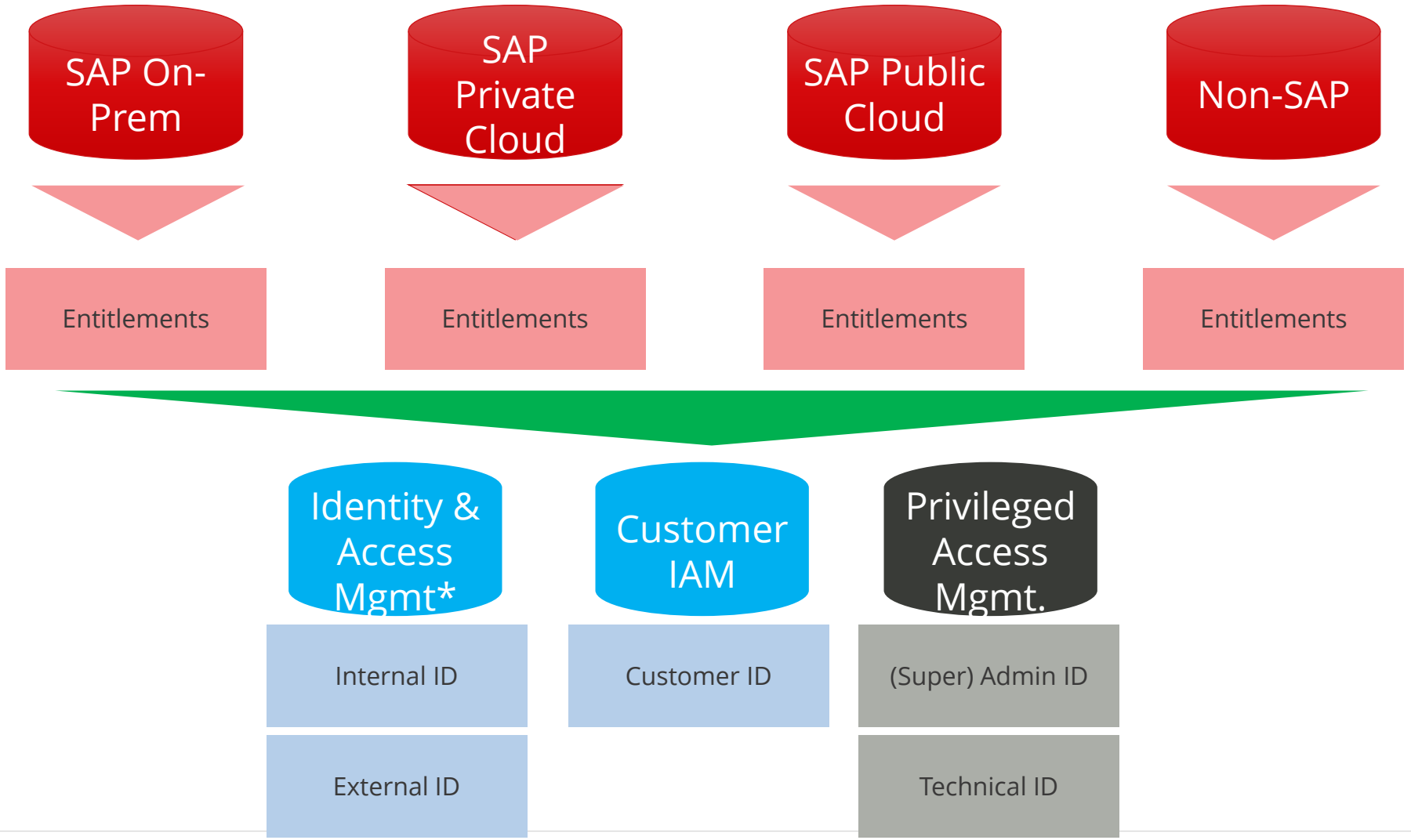
Business-Strategie

IT Strategie

Fachbereich

IT Services

Systemspezifische Entitlements können zu zentralen IDs zugeordnet werden



ID = Identität
(natürliche Person oder technisch)

Paricon vereinfacht die Verwaltung von schützenswerten Daten

Problemstellung

- Der Fachbereich ist stark eingebunden
- Es sind nur geringe Aufwände für die Implementierung verfügbar
- Schnelle Verarbeitungszeit
- Konsistente Anonymisierung

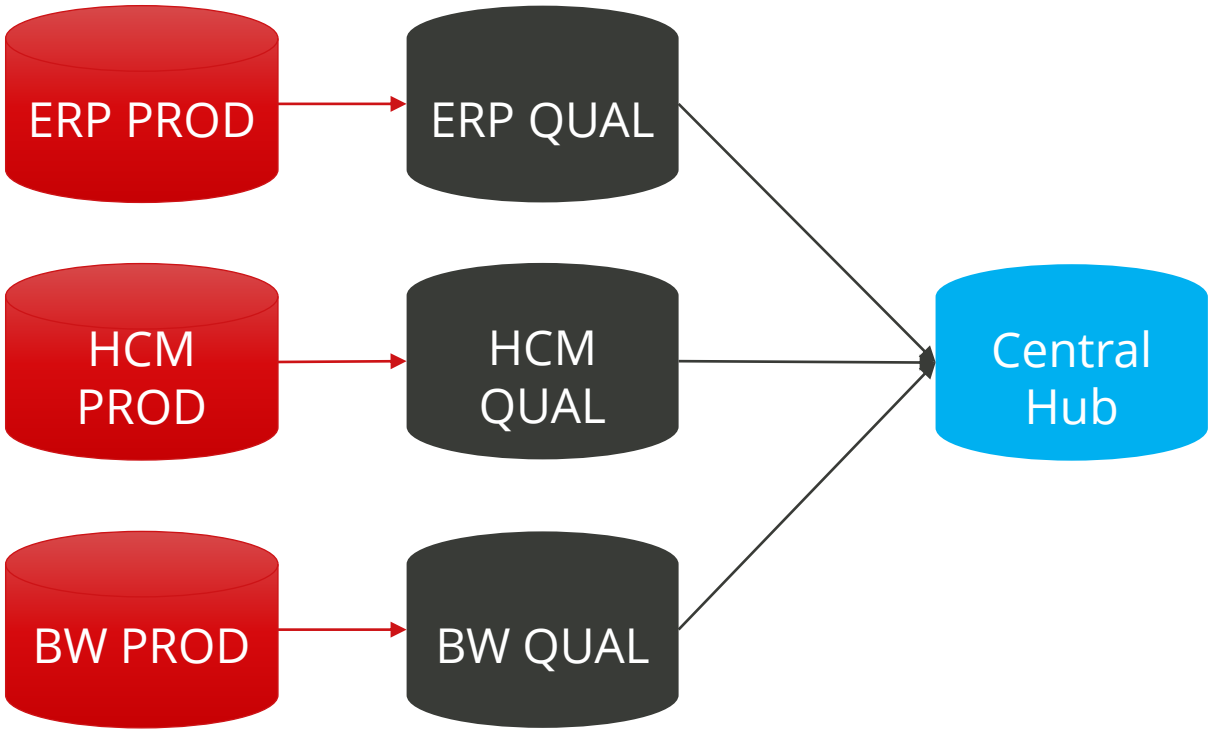
Herausforderungen

- Großzügige Rechtevergabe
- Zugriff durch externe Mitarbeiter
- Unzureichende Absicherung
- Relevante unstrukturierte Daten (Langtexte, IDOCs, Freitextfelder)
- Viele Nutzergruppen
- Daten müssen nah am produktiven Betrieb sein

Lösungsansatz mit Paricon

1. Robo-Crawler basierte Identifizierung aller schutzwürdigen und kritischen Informationen
2. Intelligente Suchalgorithmen
3. Durchführung der Anonymisierung bzw. des Löschvorgangs auf dem Zielsystem
4. Nachvollziehbarkeit durch umfassende Protokollierung

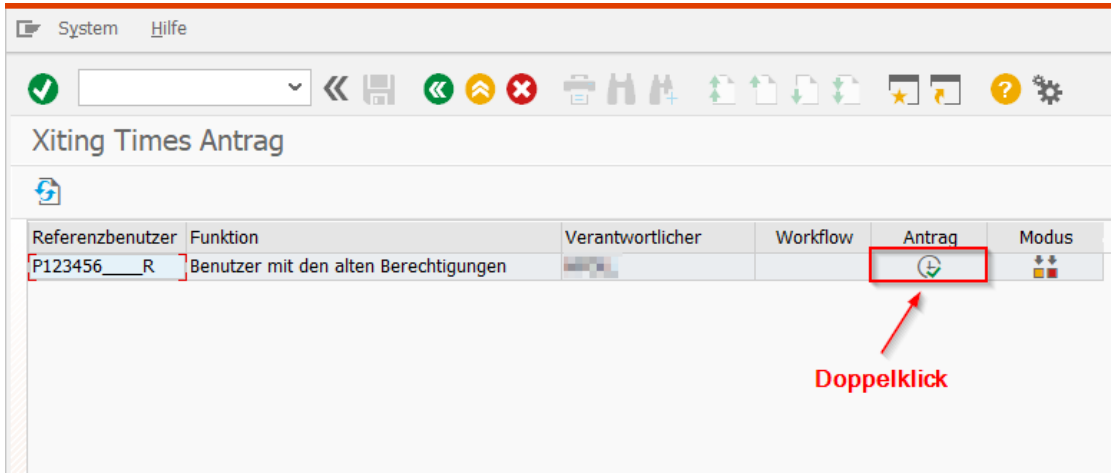
Das Paricon Central Hub ermöglicht eine zentrale Datenanonymisierung

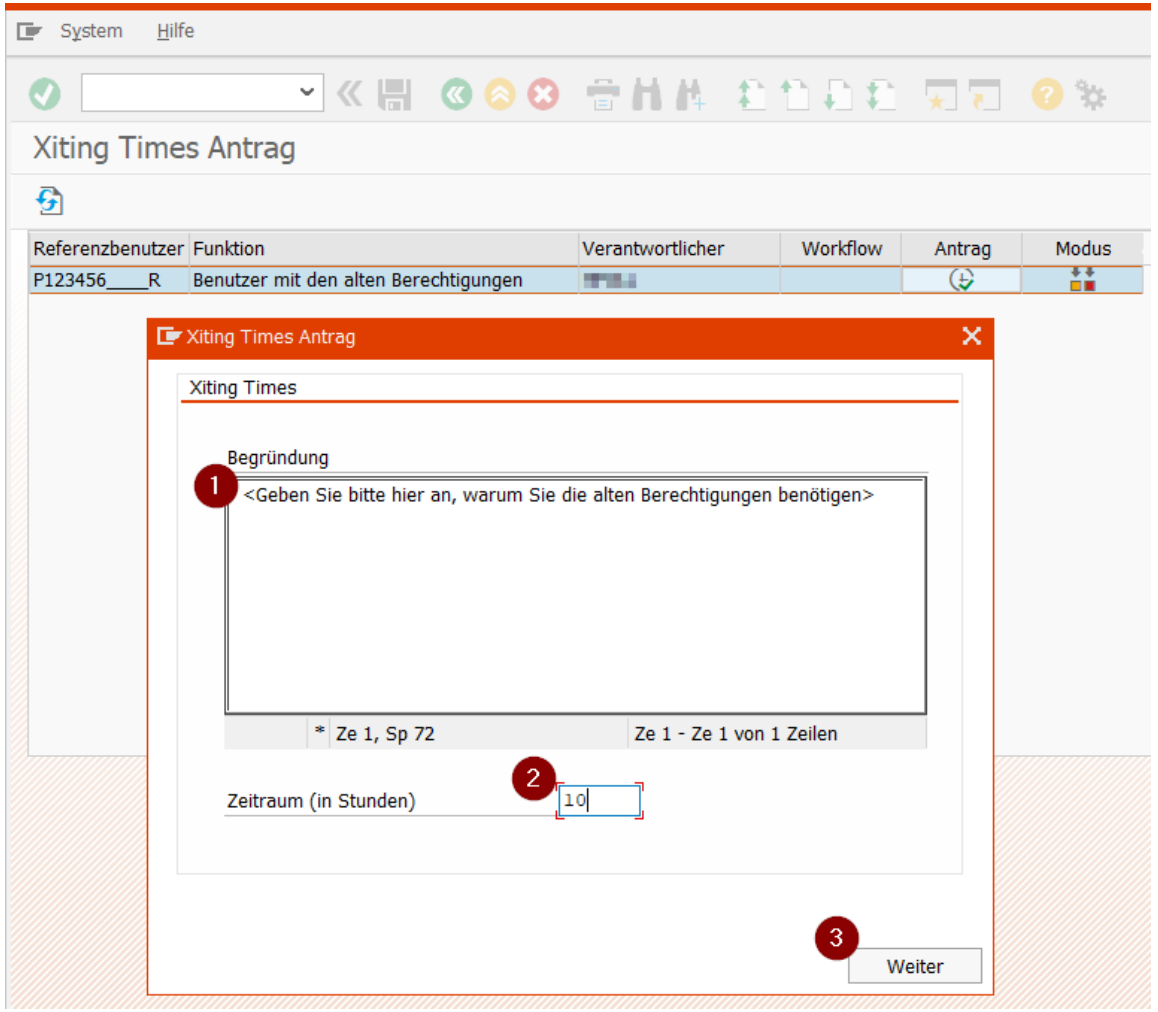


Zentrale Datenanonymisierung & Datenbereinigung (z.B. im Solman):

- Übersicht über schutzrelevante Informationen (Anzahl Tabellen/ Felder, letzte Verschlüsselung, letzte Bereinigung)
- Parametrisierung der Analyse, Anonymisierung und Bereinigung (systemübergreifend & systemspezifisch)
- Ausführung & Überwachung der Analyse-, Anonymisierungs-, und Bereinigungsläufe

Fachbereich & Test Team können durch Protected Go-Life entlastet werden





Der Aufwand für Zuweisungen kann durch Role Mining reduziert werden

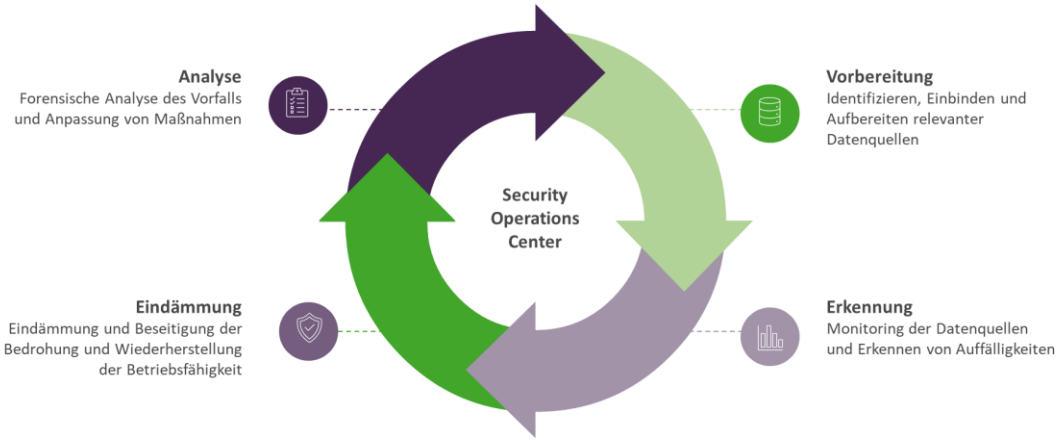
- Rechtevergaben können auf unterschiedliche Weise erfolgen
  - Explizit durch manuelle Zuweisung
  - Implizit durch andere User Attribute
  - Per Default
- Eine Erhöhung der per „default“ bzw. implizit zugewiesenen Rechte reduziert den Aufwand für explizite Zuweisungen dramatisch
- Eine Rolle ist lediglich ein weiteres User Attribut, es kann per Default oder auch implizit auf Basis anderer User Attribute vergeben werden
- Role Mining kann die Aufwände für explizite Rechtevergaben reduzieren

Ein SIEM Connector bildet das Fundament für Secure Operations

Menschen
Erledigen die Aufgaben eines SOC.

Technologien
Unterstützen Menschen entlang der Prozesse.

Prozesse
Strukturieren die Aufgaben eines SOC.

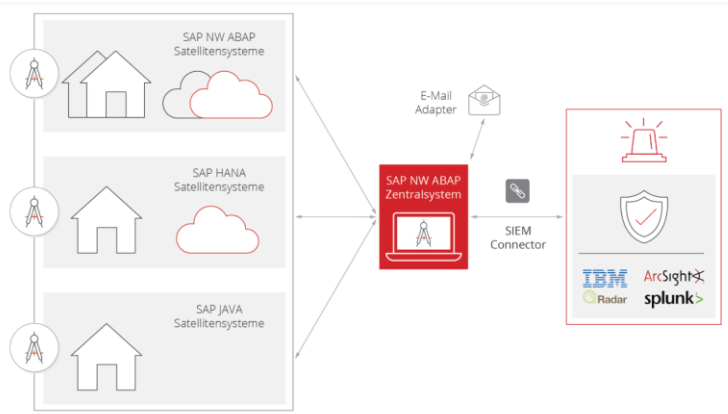


Analyse
Forensische Analyse des Vorfalls und Anpassung von Maßnahmen

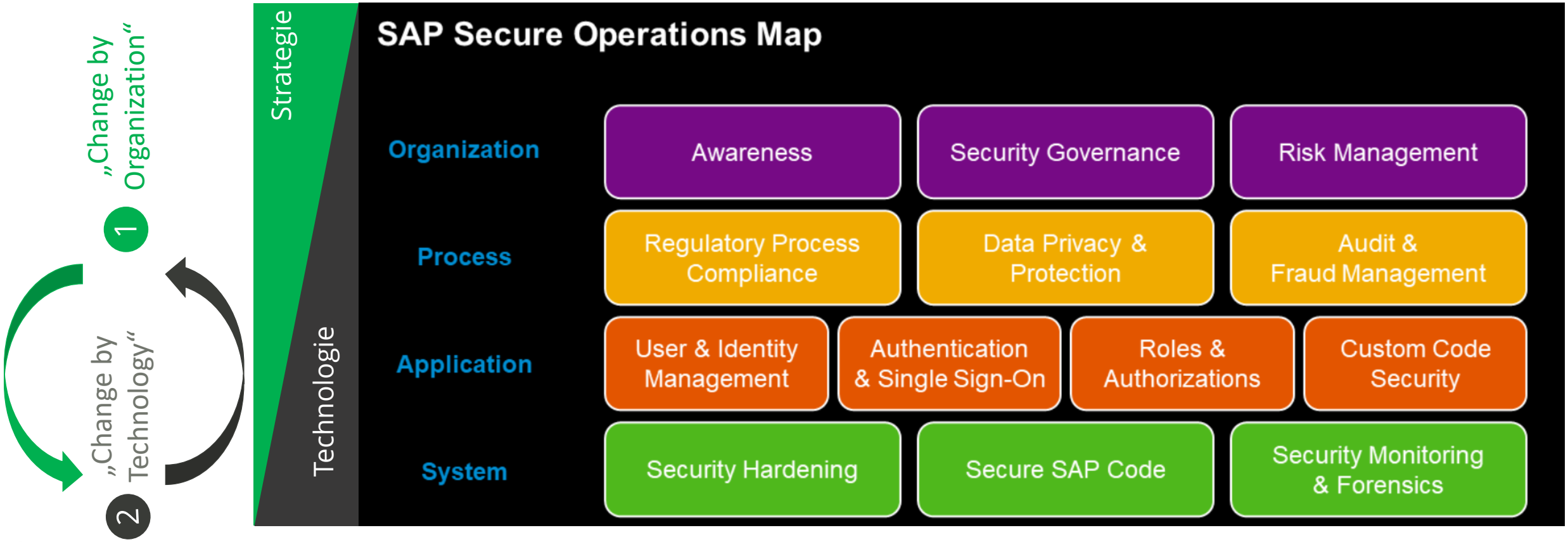
Vorbereitung
Identifizieren, Einbinden und Aufbereiten relevanter Datenquellen

Eindämmung
Eindämmung und Beseitigung der Bedrohung und Wiederherstellung der Betriebsfähigkeit

Erkennung
Monitoring der Datenquellen und Erkennen von Auffälligkeiten



Die SAP Secure Operations Map zeigt weitere Handlungsfelder auf



Wir wollen Ihre SAP Security Projekte strategisch absichern

PERIOR

2 „Change by Technology“

Strategic Alignment Model

Ihr Business

Technologie

1 „Change by Organization“

Strategie

Ihr operativer Betrieb

Business-Strategie

- Alleinstellungs-merkmale & Vorteile
- Geschäftsmodell & Marktumfeld
- Unternehmens-Kooperationen

IMS | SAFe | Scrum ban | CCoE

Fachbereich

- Hierarchische bzw. agile Organisation & Skillset
- Geschäftsprozesse & Arbeitsmodelle

IT Strategie

- IT-Services & Architektur
- IT-Organisation & Skill-Set
- IT-Kooperationen

ITing quality | ibs Schreiber | SAP S/4 HANA | paricon | u.v.m...

IT Services

- Hierarchische bzw. agile Organisation & zentrale bzw.. dezentrale Governance
- DevSecOps
- IT-System & Platform

IMS = Integriertes Mgmt. System
SAFe = Scaled Agile Framework
CCoE = Competence Center of Excellence

Kapitel 4

Golden Circle

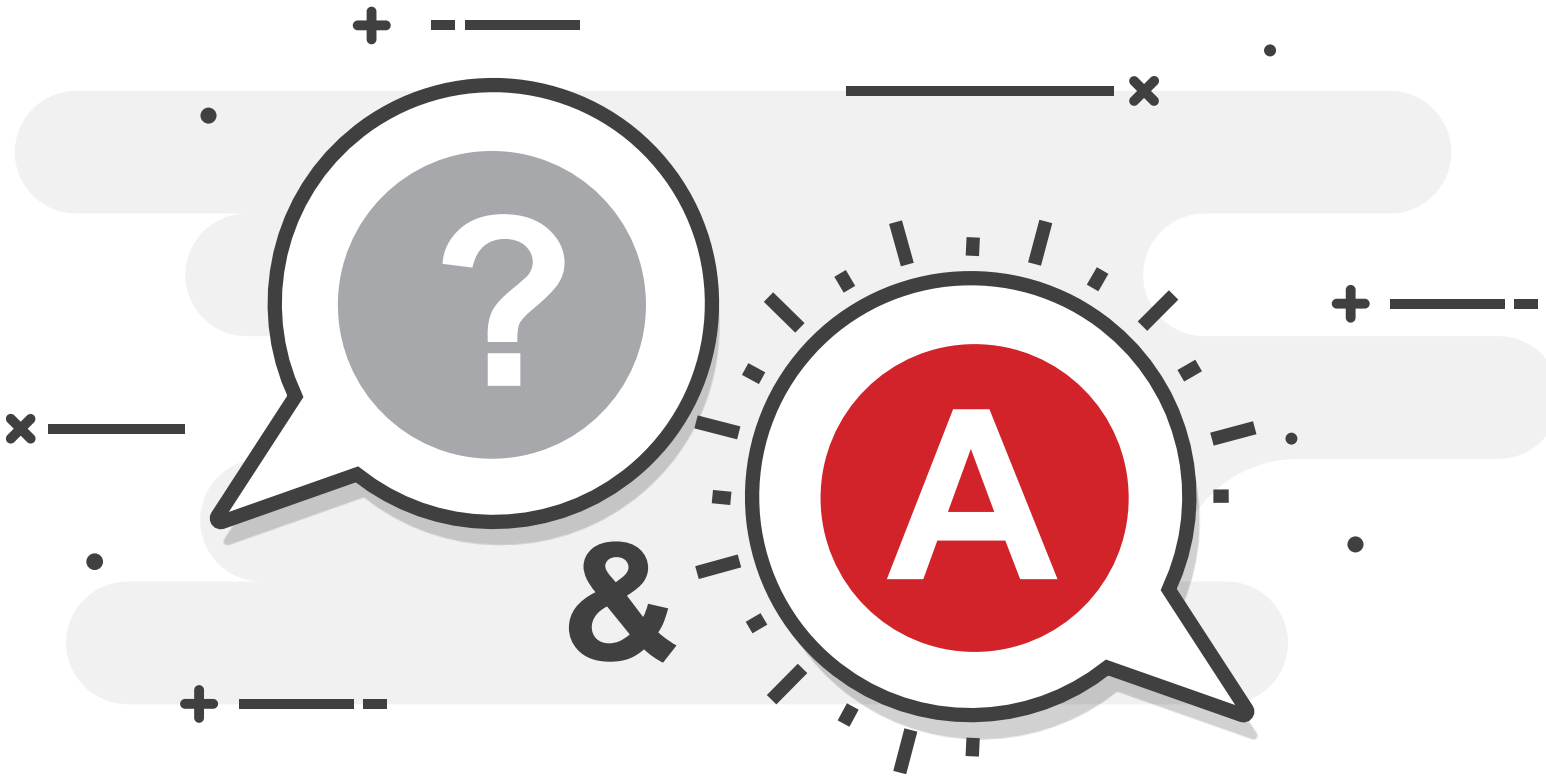
Bitte das „Why“, „How“ & „What“ Ihrer SAP Security Vision am Flipchart erarbeiten

1. **Why**
   - Warum wollen Sie Ihre SAP Security Vision verwirklichen?
     - Organisatorisch
     - Technologisch
2. **How**
   - Wie wollen Sie Ihre SAP Security Vision umsetzen?
     - Organisatorisch
     - Technologisch
3. **What**
   - Welche konkreten Aufgaben müssen Sie zur Umsetzung der SAP Security Vision umsetzen?
     - Organisatorisch
     - Technologisch

Kapitel 5

Workshop

FRAGEN UND DISKUSSIONEN



Adrian Bayer-Szegedi

Vielen Dank
Für Ihre Aufmerksamkeit

Wenn Sie weitere Informationen benötigen, können Sie mich gerne kontaktieren.