SAST

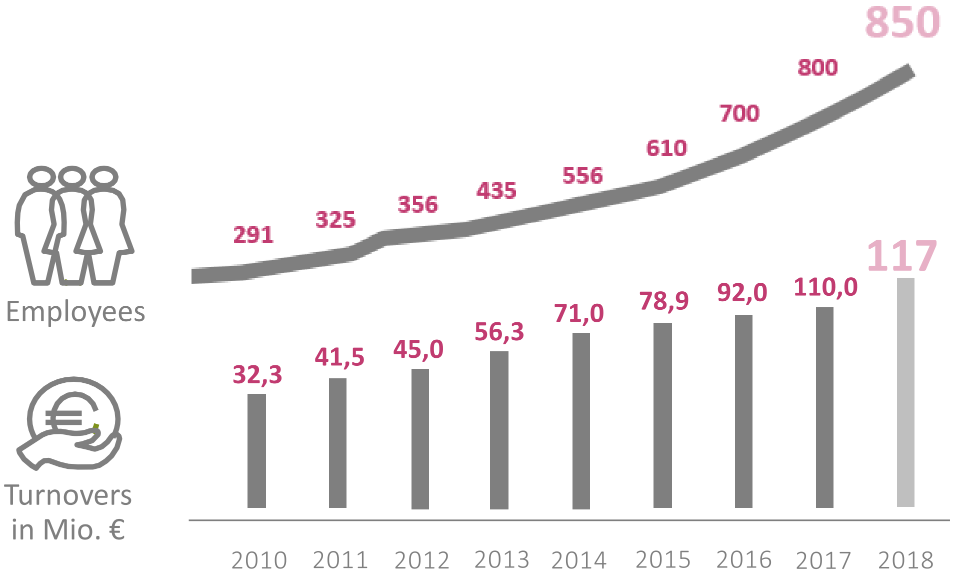
# SAP HANA & S/4HANA

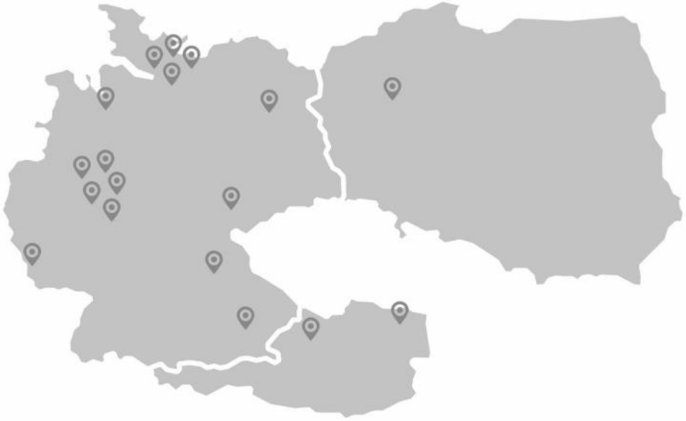
Start your SAP future securely.

# Facts and figures

AKQUINET is an international operating, continuously growing IT company headquartered in Hamburg. Our company units are organized into owner-managed midsize enterprises, which means they are both flexible and highly efficient. And as a self-financed IT business, we're independent of manufacturers and banks.

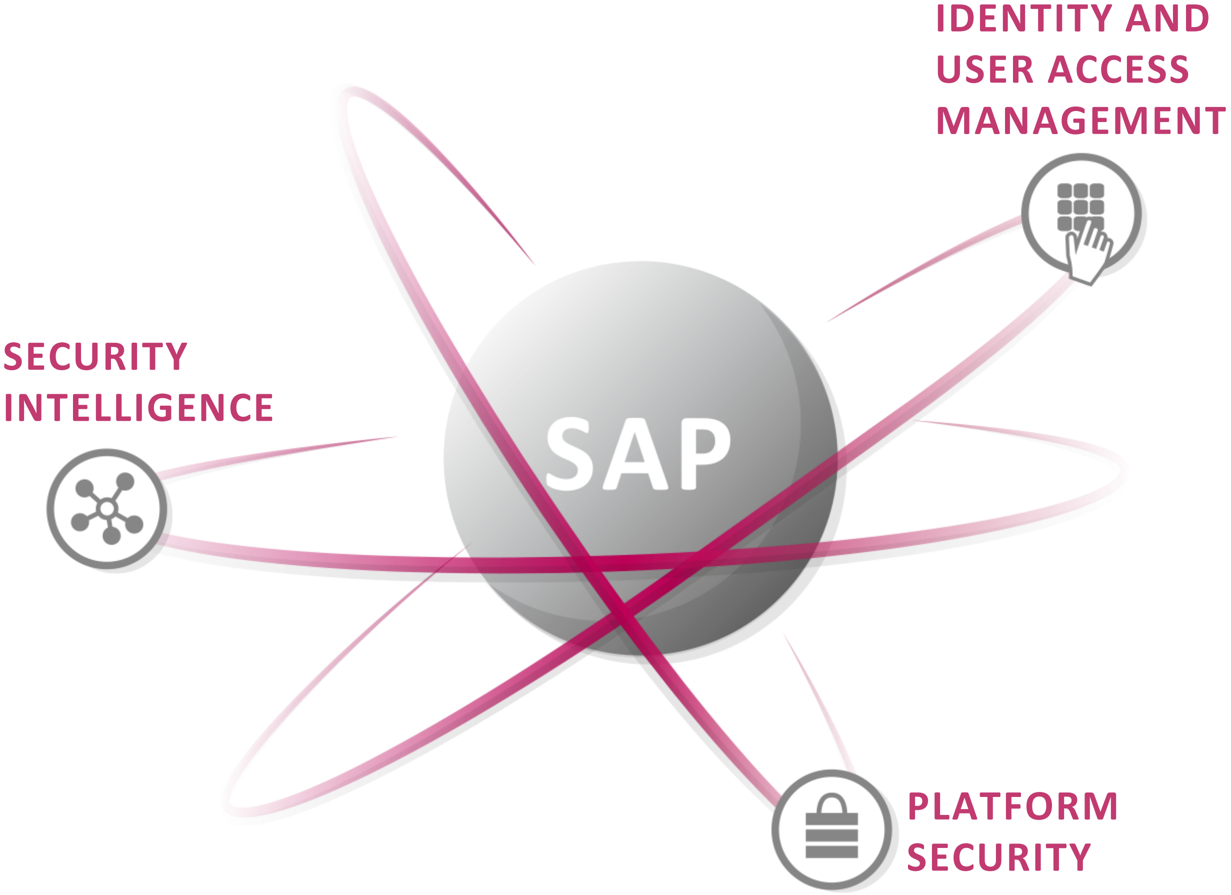
Our focus is on the introduction of ERP and S/4HANA systems, the individual development of software solutions in the areas of Java, SAP and Microsoft as well as their security.





20 offices in Germany, Austria, Poland and Brazil.
Projects in 30 countries worldwide.

# Your SAP security is our number one concern



IDENTITY AND USER ACCESS MANAGEMENT

SECURITY INTELLIGENCE

PLATFORM SECURITY

SOFTWARE

CONSULTING

MANAGED SERVICE

# Companies who´ve decided to play safe with us.

(an alphabetical listing of selected customers)

| | |
|---|---|
| Plastics | ALBIS |
| Production | amag |
| Chemical | BÆRLOCHER |
| Conglomerate | BOSCH |
| Customer goods | BRITA |
| Food | CSM Bakery Solutions |
| ICT services | DEMANDO |
| Land and housing | Deutsche Wohnen |
| Automotive | DRÄXLMAIER |
| Mechanical engineering | ENGEL |
| ICT services | finanz informatik technologie service |
| Construction | HEIDELBERGCEMENT |
| Energy | kelag |
| Machine and plant engineering | KNORR-BREMSE |
| Chemical / Textile | LENZING |
| Technology / Chemical | THE LINDE GROUP |
| Automotive | MAGNA |
| Customer goods | Miele |
| Production / Services | Brunata Minol |
| Customer goods | MONT BLANC |
| Trade | NW NORDWEST |
| Machine engineering | PALFINGER |
| Insurance | R+V |
| Trade | s.Oliver |
| Banks / Insurances | Sparkassen Versicherung |
| Pharmaceuticals | Takeda |
| Healthcare | UKE HAMBURG |
| Banks | Union Investment |
| Land and housing | VIVAWEST |
| Mining | wolfram |

# AGENDA - SAP HANA & S/4HANA

- Key messages and strategic orientation S/4HANA
- S/4HANA migration from a security point of view
- Process for a secure migration to SAP HANA DB
- Process for secure operations of S/4HANA

# Strategic orientation S/4HANA

## Decision SAP Business Suite vs. S/4HANA

- 30% of all companies will use S/4HANA as their main ERP system by 2020.
- 30% of companies have not made a decision yet.
- 40% want to stay with the traditional Business Suite until 2020.
  About half of this plan to remain on the traditional platform after 2020.

## Development in 2018

- Around 15% of all companies made a major investment in S/4HANA (on-premise) – a tripling over the previous year.
- Almost 2% of the companies are already productive with S/4HANA as their main system.
- Around 4% plan to go live during 2018.
- More than 25% intend to do so by 2020.

# Migrating from SAP ERP -> S/4HANA

## The security perspective

New installations contain security weaknesses

- Each platform contains security weaknesses "out of the box" By SAP Security Notes not implemented
- By manually set configuration settings

Security Weaknesses are being migrated to HANA

- By insecure configuration settings
- By security weaknesses in custom code

**Experience from our audits and penetration tests confirm the risks:**

! **Security guides not implemented / missing patches**

! **Missing network separation**

! **Missing monitoring**

# Migration SAP ERP -> S/4HANA

## The AKQUINET process model for a secure migration to the SAP HANA platform

**Check Security Level**

- Security audit of the target platform
- Creation of a comprehensive report of existing security vulnerabilities with recommendations for measures
- Creation of a prioritized work list as a specification for system hardening

**System Hardening**

Hardening of the systems on the levels of

- Operating system / Network
- Databases
- SAP Application Server
- Custom Code

**Security Monitoring**

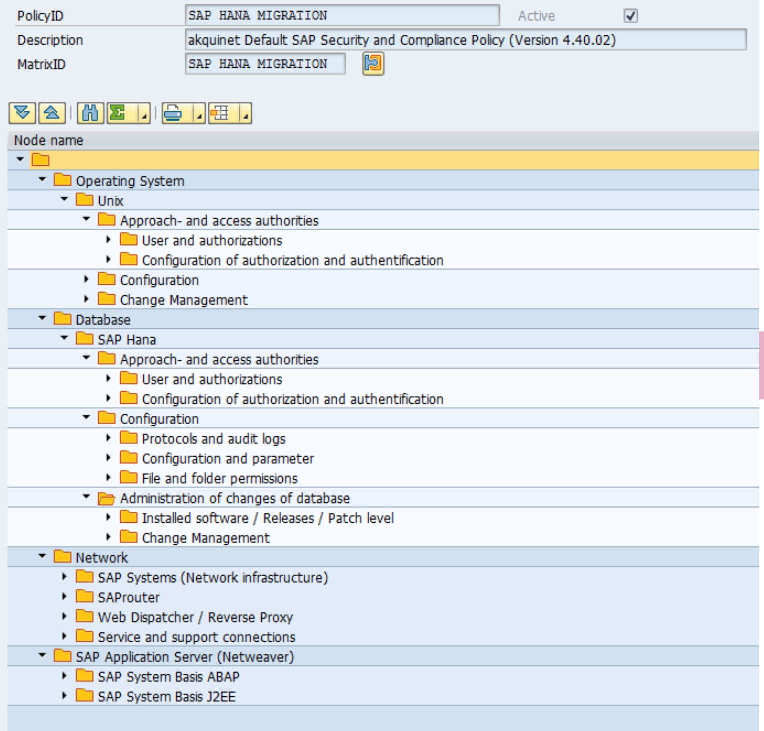
Handover hardened system

Establishing a monitoring of access at ALL levels

- Operating system / network / databases
- Basis system

# Approach for a secure operation as part of the migration to SAP HANA.

## 1. Analysis of the target platform SAP HANA with SAST System Security Validation.



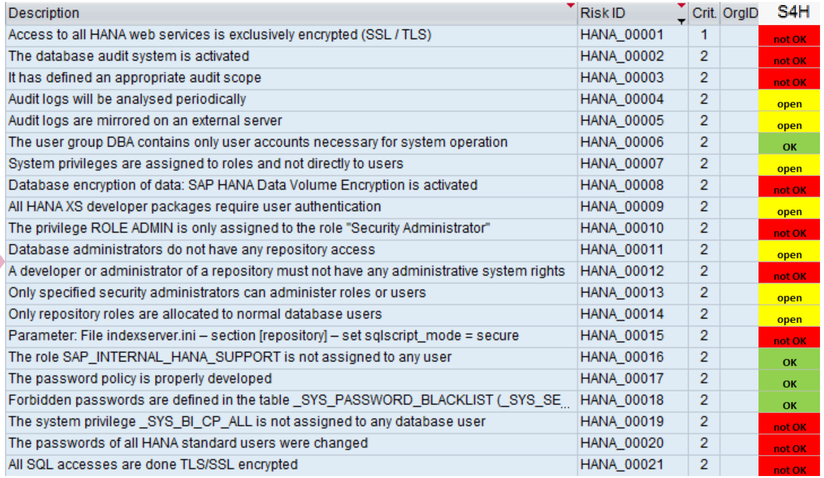
PolicyID: SAP HANA MIGRATION    Active ☑

Description: akquinet Default SAP Security and Compliance Policy (Version 4.40.02)

MatrixID: SAP HANA MIGRATION

Node name

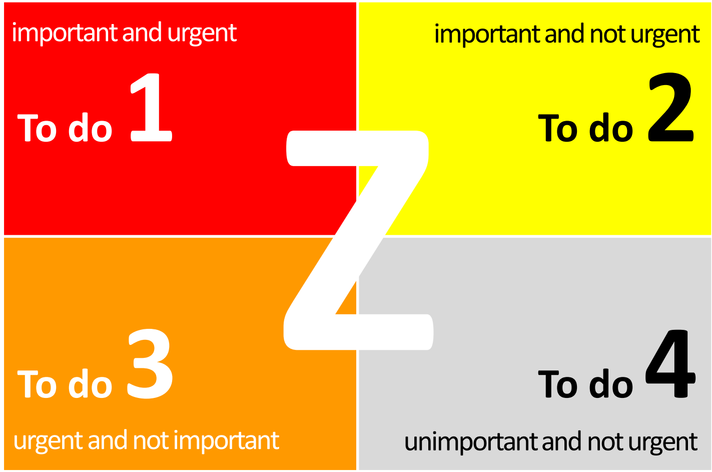
- Operating System
  - Unix
    - Approach- and access authorities
      - User and authorizations
      - Configuration of authorization and authentification
    - Configuration
    - Change Management
- Database
  - SAP Hana
    - Approach- and access authorities
      - User and authorizations
      - Configuration of authorization and authentification
    - Configuration
      - Protocols and audit logs
      - Configuration and parameter
      - File and folder permissions
    - Administration of changes of database
      - Installed software / Releases / Patch level
      - Change Management
- Network
  - SAP Systems (Network infrastructure)
  - SAProuter
  - Web Dispatcher / Reverse Proxy
  - Service and support connections
- SAP Application Server (Netweaver)
  - SAP System Basis ABAP
  - SAP System Basis J2EE



| Description | Risk ID | Crit. | OrgID | S4H |
|---|---|---|---|---|
| Access to all HANA web services is exclusively encrypted (SSL / TLS) | HANA_00001 | 1 | | not OK |
| The database audit system is activated | HANA_00002 | 2 | | not OK |
| It has defined an appropriate audit scope | HANA_00003 | 2 | | not OK |
| Audit logs will be analysed periodically | HANA_00004 | 2 | | open |
| Audit logs are mirrored on an external server | HANA_00005 | 2 | | open |
| The user group DBA contains only user accounts necessary for system operation | HANA_00006 | 2 | | OK |
| System privileges are assigned to roles and not directly to users | HANA_00007 | 2 | | open |
| Database encryption of data: SAP HANA Data Volume Encryption is activated | HANA_00008 | 2 | | not OK |
| All HANA XS developer packages require user authentication | HANA_00009 | 2 | | open |
| The privilege ROLE ADMIN is only assigned to the role "Security Administrator" | HANA_00010 | 2 | | not OK |
| Database administrators do not have any repository access | HANA_00011 | 2 | | open |
| A developer or administrator of a repository must not have any administrative system rights | HANA_00012 | 2 | | not OK |
| Only specified security administrators can administer roles or users | HANA_00013 | 2 | | open |
| Only repository roles are allocated to normal database users | HANA_00014 | 2 | | open |
| Parameter: File indexserver.ini – section [repository] – set sqlscript_mode = secure | HANA_00015 | 2 | | not OK |
| The role SAP_INTERNAL_HANA_SUPPORT is not assigned to any user | HANA_00016 | 2 | | OK |
| The password policy is properly developed | HANA_00017 | 2 | | OK |
| Forbidden passwords are defined in the table _SYS_PASSWORD_BLACKLIST (_SYS_SE... | HANA_00018 | 2 | | OK |
| The system privilege _SYS_BI_CP_ALL is not assigned to any database user | HANA_00019 | 2 | | not OK |
| The passwords of all HANA standard users were changed | HANA_00020 | 2 | | not OK |
| All SQL accesses are done TLS/SSL encrypted | HANA_00021 | 2 | | not OK |

# Approach for a secure operation as part of the migration to SAP HANA

## 2. Preparation for hardening the target platform SAP HANA



important and urgent

To do 1

important and not urgent

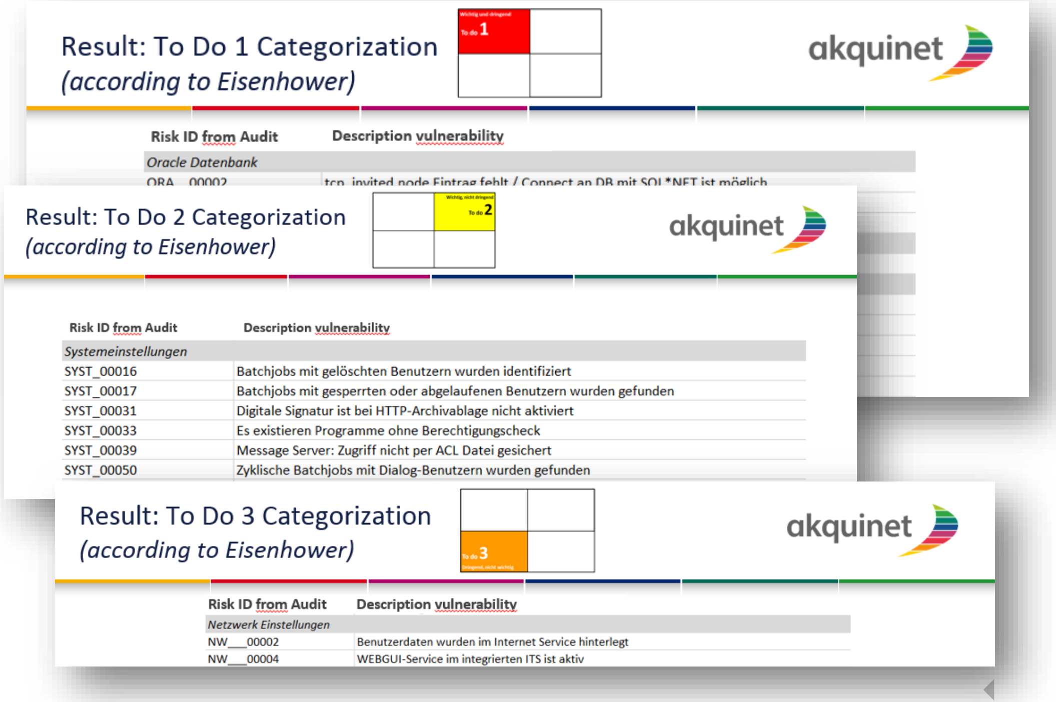
To do 2

To do 3

urgent and not important

To do 4

unimportant and not urgent



### Result: To Do 1 Categorization *(according to Eisenhower)*

| Risk ID from Audit | Description vulnerability |
|---|---|
| *Oracle Datenbank* | |
| ORA__00002 | tcp_invited node Eintrag fehlt / Connect an DB mit SQL*NET ist möglich |

### Result: To Do 2 Categorization *(according to Eisenhower)*

| Risk ID from Audit | Description vulnerability |
|---|---|
| *Systemeinstellungen* | |
| SYST_00016 | Batchjobs mit gelöschten Benutzern wurden identifiziert |
| SYST_00017 | Batchjobs mit gesperrten oder abgelaufenen Benutzern wurden gefunden |
| SYST_00031 | Digitale Signatur ist bei HTTP-Archivablage nicht aktiviert |
| SYST_00033 | Es existieren Programme ohne Berechtigungscheck |
| SYST_00039 | Message Server: Zugriff nicht per ACL Datei gesichert |
| SYST_00050 | Zyklische Batchjobs mit Dialog-Benutzern wurden gefunden |

### Result: To Do 3 Categorization *(according to Eisenhower)*

| Risk ID from Audit | Description vulnerability |
|---|---|
| *Netzwerk Einstellungen* | |
| NW___00002 | Benutzerdaten wurden im Internet Service hinterlegt |
| NW___00004 | WEBGUI-Service im integrierten ITS ist aktiv |

# Procedure for a secure operation as part of the migration to SAP HANA

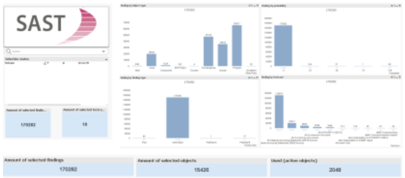
## 3. Implementation of system hardening

- Coordination of the work list with the responsible persons
- Execution of system hardening acc. prioritized work list, providers instructions for secure operations and the AKQUINET Best Practice-Recommendations
    - Handover of the hardened system
- Clean Up Custom Code
    - Define relevant code areas
    - Intelligent Code Analysis // Use Context information
    - Lock/eliminate inactive objects
- Soft-Cleansing of Custom Code findings
- Establishment of monitoring accesses at ALL levels e.g. with the SAST Security Radar

# Reduce effort for HANA migrations with SAST Code Security Advisory

## 1. ABAP-Code Scan

## 2. Soft Code Cleansing



Amount of selected findi...

170282

Amount of selected tech o...

18

Amount of selected findings

170282

Amount of selected objects

15426

Used (active objects)

2048

- ✓ Indentify and block unused ERP customer code.
- ✓ Minimize operational risks due to „Soft Cleaning“.
- ✓ Code cleansing 80% cheaper. Reduce HANA migration costs.

# MASTER THE ROLE MIGRATION SECURELY WITH US.

SAP-Security for S/4HANA

# What should be considered during the migration?

## Redesign your authorizations for S/4HANA

- **Why is a new authorization concept necessary?**
  - SAP S/4HANA is the new software suite of SAP and not just an evolution of SAP ERP.
  - Authorization concepts from ERP can not be transferred without adaptation.
  - Some transactions are obsolete
- **What actions are necessary to convert your authorizations?**
  - Examination & Redesign of existing roles and processes and/or creation of new roles.
  - Check roles for critical authorizations and SoD risks.
  - Update of SU24 values to SAP S/4HANA.
  - Configuration of SAP Fiori apps.

**Without a redesign** of your authorization concept, **no migration** is possible.

# Possible solutions

## The chosen approach strongly depends on the quality of the roles and the internal objectives:

### Transformation of existing roles from the legacy system

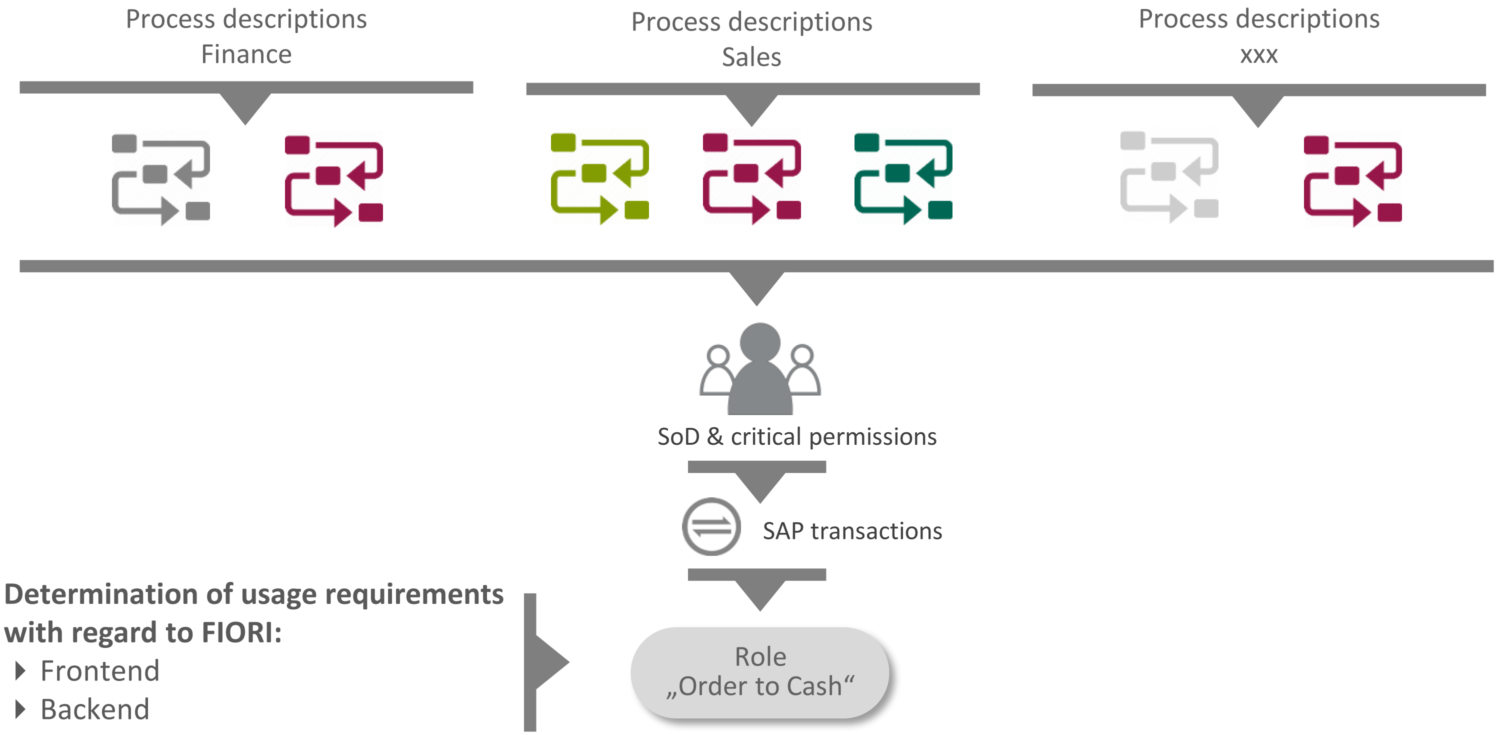
- Documented process role model
- Automatic adaptation with SAST Suite 5.0
- S/4HANA conversion tools
- Small manual rework
- Test support with SAST Safe Go-Live

### New authorizations for S/4HANA

- Rebuilding a process role model based on the AKQUINET best practice approach in combination with the SAST 5.0 authorization trace
- Using the AKQUINET role templates for S/4HANA
- Test support with SAST Safe Go-Live

# Concept proposal: "Authorization Redesign"

## Process-oriented role concept based on process descriptions and "stories"



Process descriptions Finance

Process descriptions Sales

Process descriptions xxx

SoD & critical permissions

SAP transactions

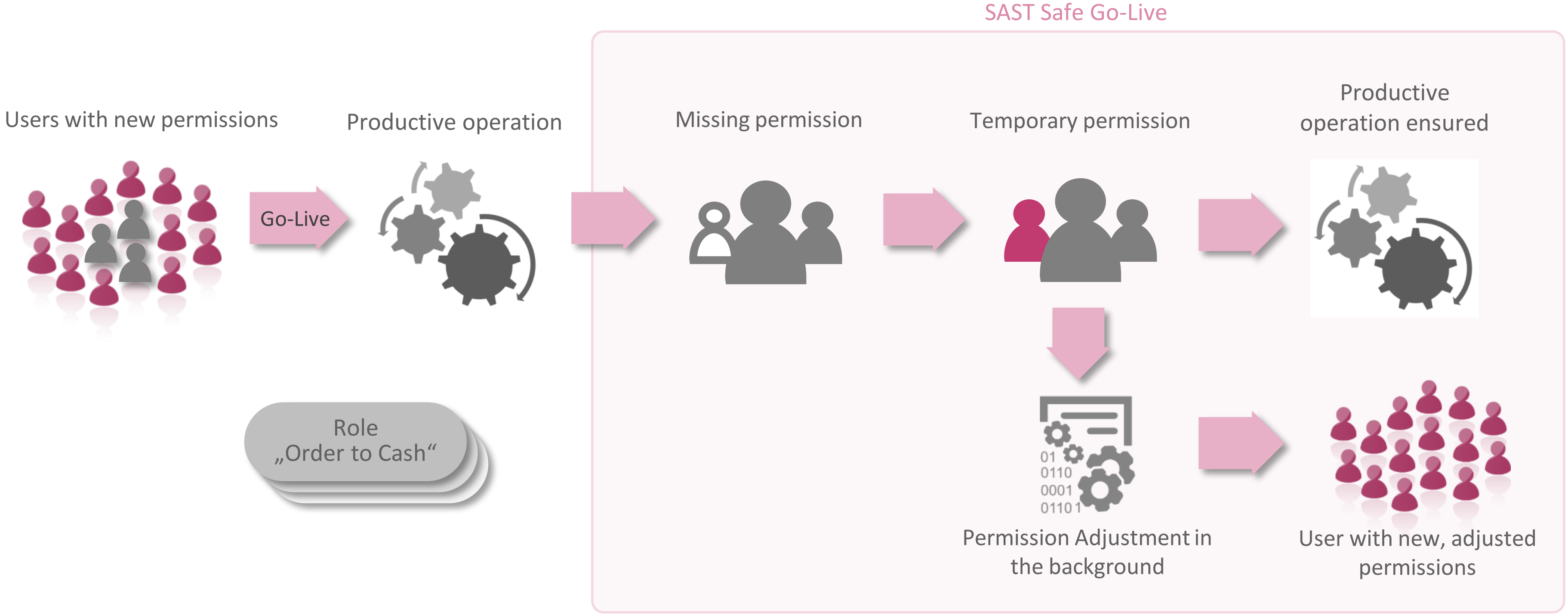
Role „Order to Cash“

**Determination of usage requirements with regard to FIORI:**

- Frontend
- Backend

# Concept proposal: "Authorization Redesign"

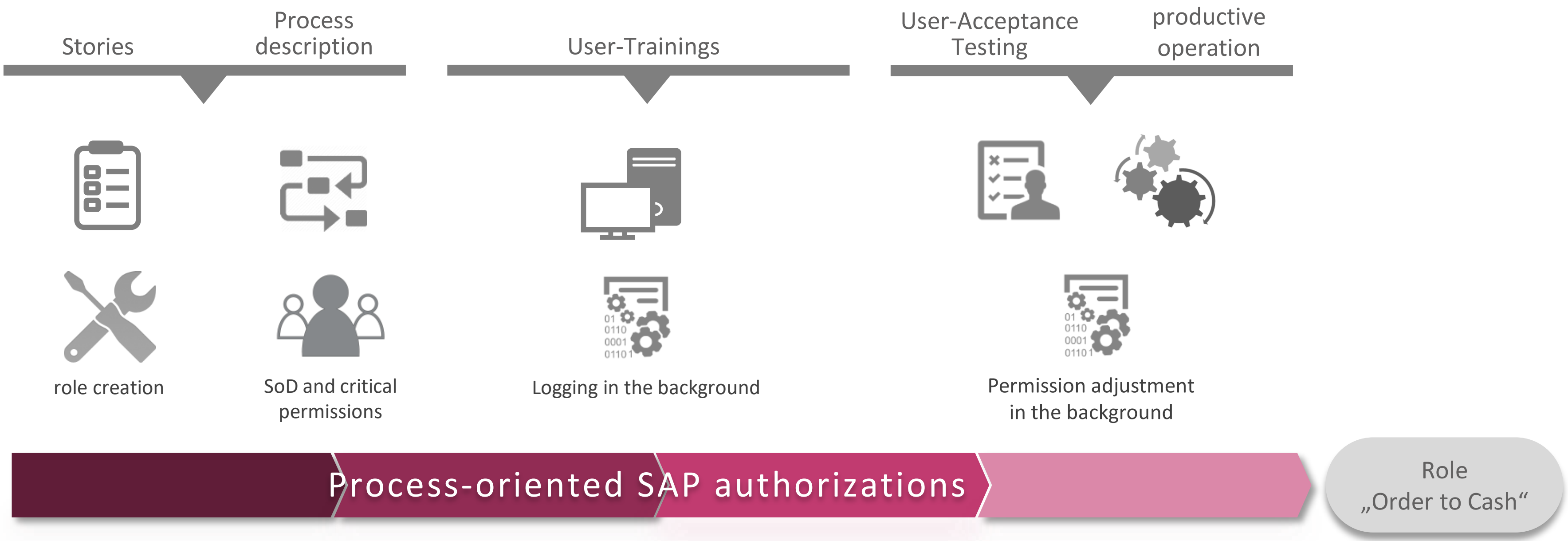
## Safe go-live procedure with "fallback option"


SAST Safe Go-Live
Users with new permissions
Go-Live
Productive operation
Role „Order to Cash“
Missing permission
Temporary permission
Productive operation ensured
01 0110 0001 01101
Permission Adjustment in the background
User with new, adjusted permissions

✓ By using the "fallback option“, productive operation is not affected at any time!

# Concept proposal: "Authorization Redesign"

## Development stages of new process-oriented SAP authorizations for S / 4HANA



Stories

Process description

User-Trainings

User-Acceptance Testing

productive operation

role creation

SoD and critical permissions

Logging in the background

Permission adjustment in the background

Process-oriented SAP authorizations

Role „Order to Cash“

✓ Using the **SAST role templates** to support role building, SAP authorizations are created process-oriented in a rolling process.

# DO YOU HAVE ANY QUESTIONS?
# WE ANSWER. FOR SURE.

**RALF KEMPF**
Technical Managing Director SAST SOLUTIONS

- More than 20 years of experience in SAP security services and software development
- Specializing in security analysis and testing of complex SAP systems
- Architect of the AKQUINET SAST SUITE

| | |
|---|---|
| Mobil: | +49 172 4435653 |
| Email: | ralf.kempf@akquinet.de |
| Web: | www.sast-solutions.com |