

# SAP Security & Compliance Audits.

Find your vulnerabilities before you get hurt.



# WELCOME!

Introducing your host today:



**TIM KRÄNZKE**

Member of the Executive Board

Fon: +49 40 88173-2735  
Email: [tim.kraenzke@akquinet.com](mailto:tim.kraenzke@akquinet.com)  
Web: [sast-solutions.com](http://sast-solutions.com)



**AXEL GIESE**

Senior Consultant SAP Security

Fon: +49 40 88173-2709  
Email: [axel.giese@akquinet.com](mailto:axel.giese@akquinet.com)  
Web: [sast-solutions.com](http://sast-solutions.com)

**„From our project experiences we know:  
every system is vulnerable. It is a question of  
how difficult it is and how long it takes.**

We rarely find SAP systems in which the infrastructure is hardened in the best possible way and effective authorization management is lived out.

Threats are almost always detected too late.

With the right concept, the probability of a successful attack can be significantly reduced.“



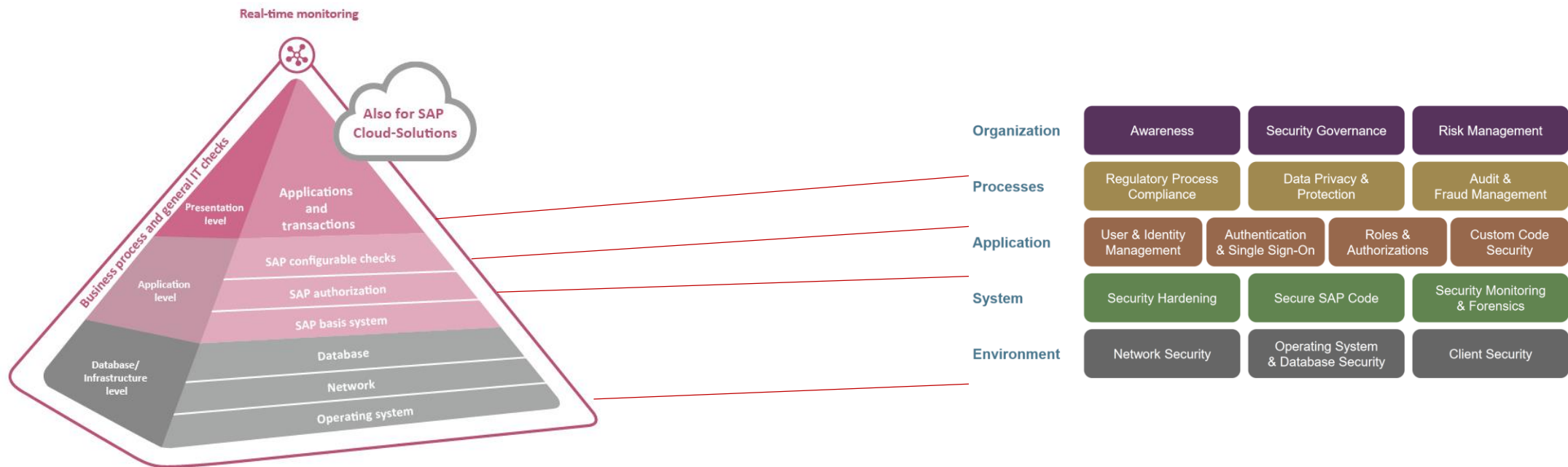
**Ralf Kempf**

CTO SAST SOLUTIONS

# Scope of safty tests

A meaningful audit should consider the following aspects:

- ▶ Comprehensiveness
- ▶ Systematics
- ▶ Assignment to system landscapes
- ▶ Consideration of specific customer situations



SAP security and compliance know-how for your digital future :

## SAST CONSULTING for SAP ERP and S/4HANA



### SAP SECURITY CONSULTING

Security & Compliance Audits

Penetration Tests

System Hardening & Optimization

SAP Security Guidelines

Source Code Analysis & Cleansing



### SAP AUTHORIZATION CONSULTING

Pilot Studies

Authorization Concepts

Roles & Authorization Optimization

S/4HANA Migration

GRC Workshops

# 4D IT-SECURITY: Comprehensive protection in real-time!

## Our process model

### Security Level Validation

- Security assessment / Audit
- Penetration test

### System Hardening

- System hardening on ALL levels
- OS / Network / Databases
  - Basis system / Authorizations / Configurable controls
  - Applications and transactions

### Security Monitoring

- Access monitoring on ALL levels
- OS / Network / Databases
  - Basis system / Authorizations / Configurable controls
  - Applications and transactions



## Passive Testing

### Security / Vulnerability Assessment (Quick Check)

- ▶ Analysis of the test object for security deficiencies.
- ▶ Use of automated tools.
- ! Objective: Identify ALL possible vulnerabilities.

### IT Security und Compliance Audit

- ▶ Target/actual comparison of the test object: in-/external guidelines (BSI, ISO, SOX, PCI) or "state of the art".
- ▶ Analysis of the test object for security deficiencies and deviations from standards.
- ! Objective: Validating processes, documentation and systems against guidelines.



## Active Testing

### Penetration Test

- ▶ Testing of IT components regarding the existence and effectiveness of security measures and active exploitation of weak points.
- ! Objective: Analysis of the system and break-in through active use of vulnerabilities.

## Benefits



### Authorizations

### Development/ Customizing

### Systemconfig./ Operations

#### Business Departments

Through extensive analyses of the critical authorizations and SoD conflicts in various modules and processes (HR, FI/CO, P2P, O2C, etc.), misconduct in the authorization management can be found and subsequently eliminated in order to meet legal and internal requirements.



#### Basis / IT Department

The SAST Quick Check examines authorizations in the IT basis environment in more detail and examines them for SoD conflicts. In addition to the security-relevant system settings and parameters, various developments and customizing settings are also checked regarding their system security.



#### Control Instances

Analyses by the SAST Quick Check can support different control instances such as internal or external audits and lead to cost savings.

# Use case: Migration SAP ERP / AnyDB -> SAP HANA & S/4HANA

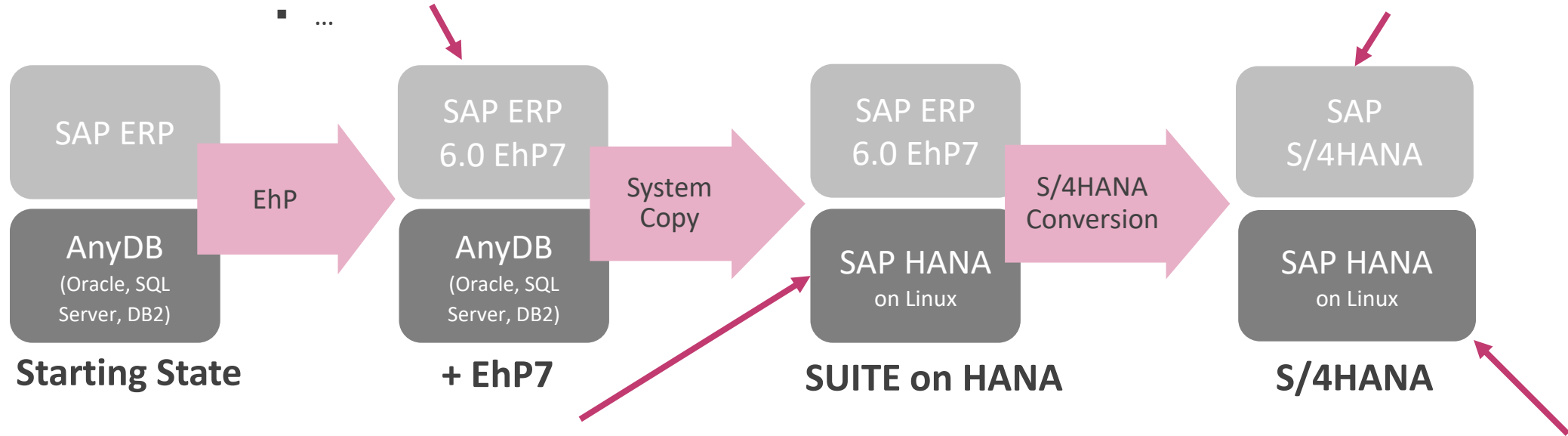
A good time for a safety check.

## 1. Security Gap: Application Server

- Parameter
- Auditing
- Security Patches
- ...

## 4. Security Gap: S/4HANA Authorizations

- Critical Authorizations
- SoD Conflicts



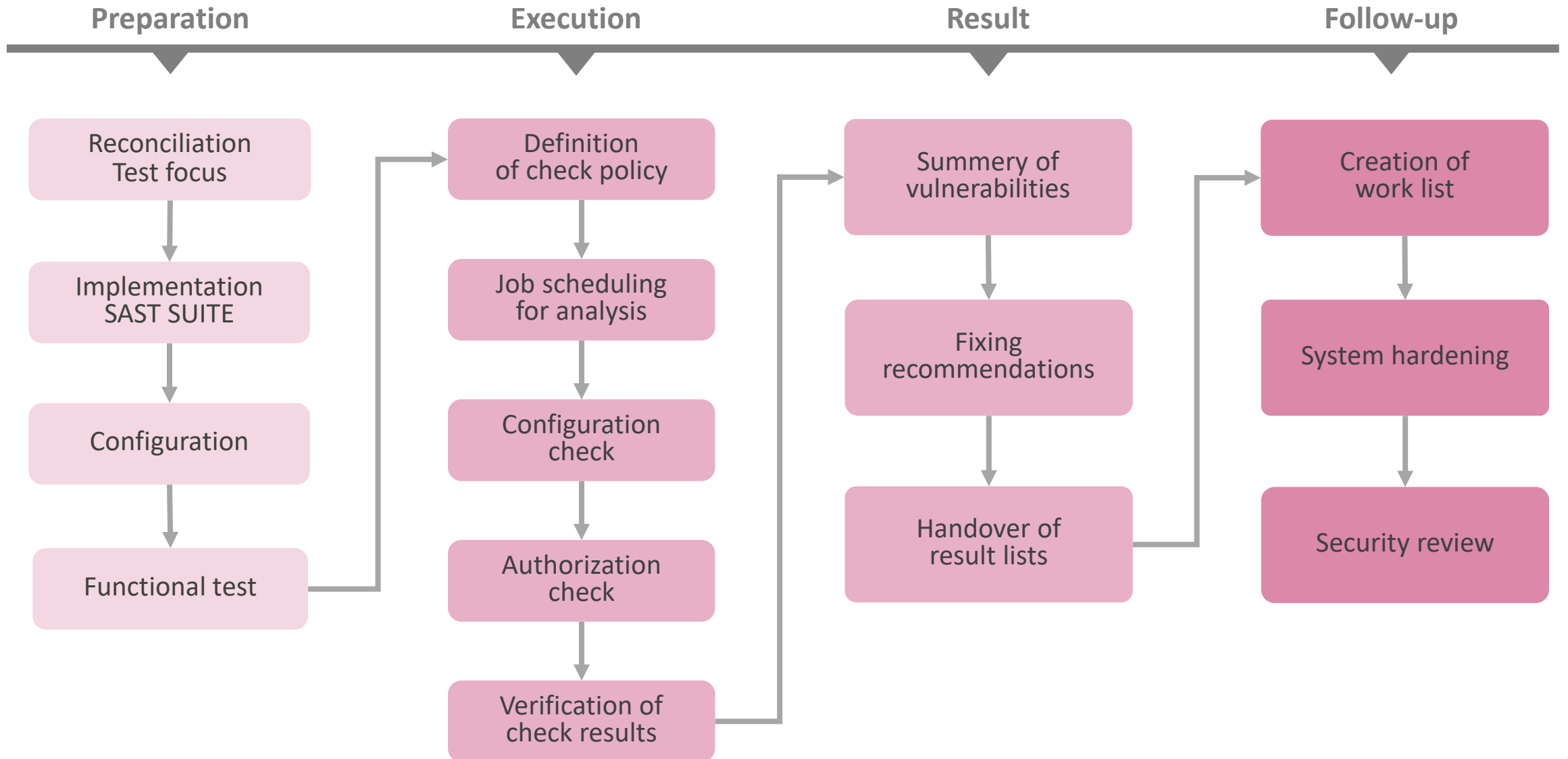
## 2. Security Gap: Operating System

- Authentication Settings
- Network Settings
- Service and File Permissions
- Logging and Reporting
- ...

## 3. Security Gap: Database

- Authentication Parameters
- HANA Authorizations
- Audit Settings
- Security Patches
- ...

# Procedure of Security / Vulnerability Assessments (Quick Check):



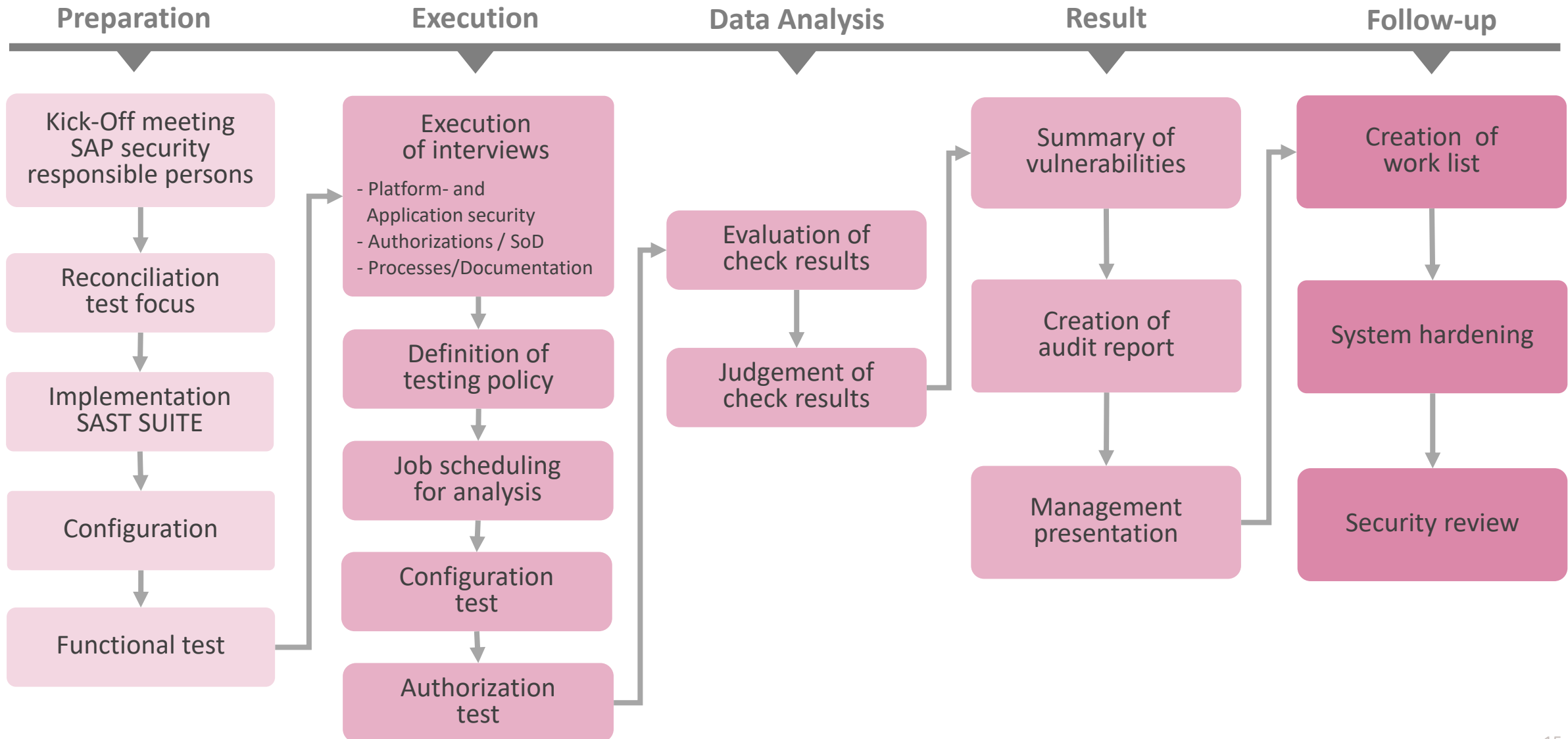
**“Thanks to the SAP Security Quick Audit conducted by the SAST team, we have identified the areas where we need to take action in order to meet the requirements of the IT security law.”**



**ST. GEORG  
KLINIKUM  
EISENACH**

**- Michael Trautwein -**

# Procedure of IT Security and Compliance Audits:



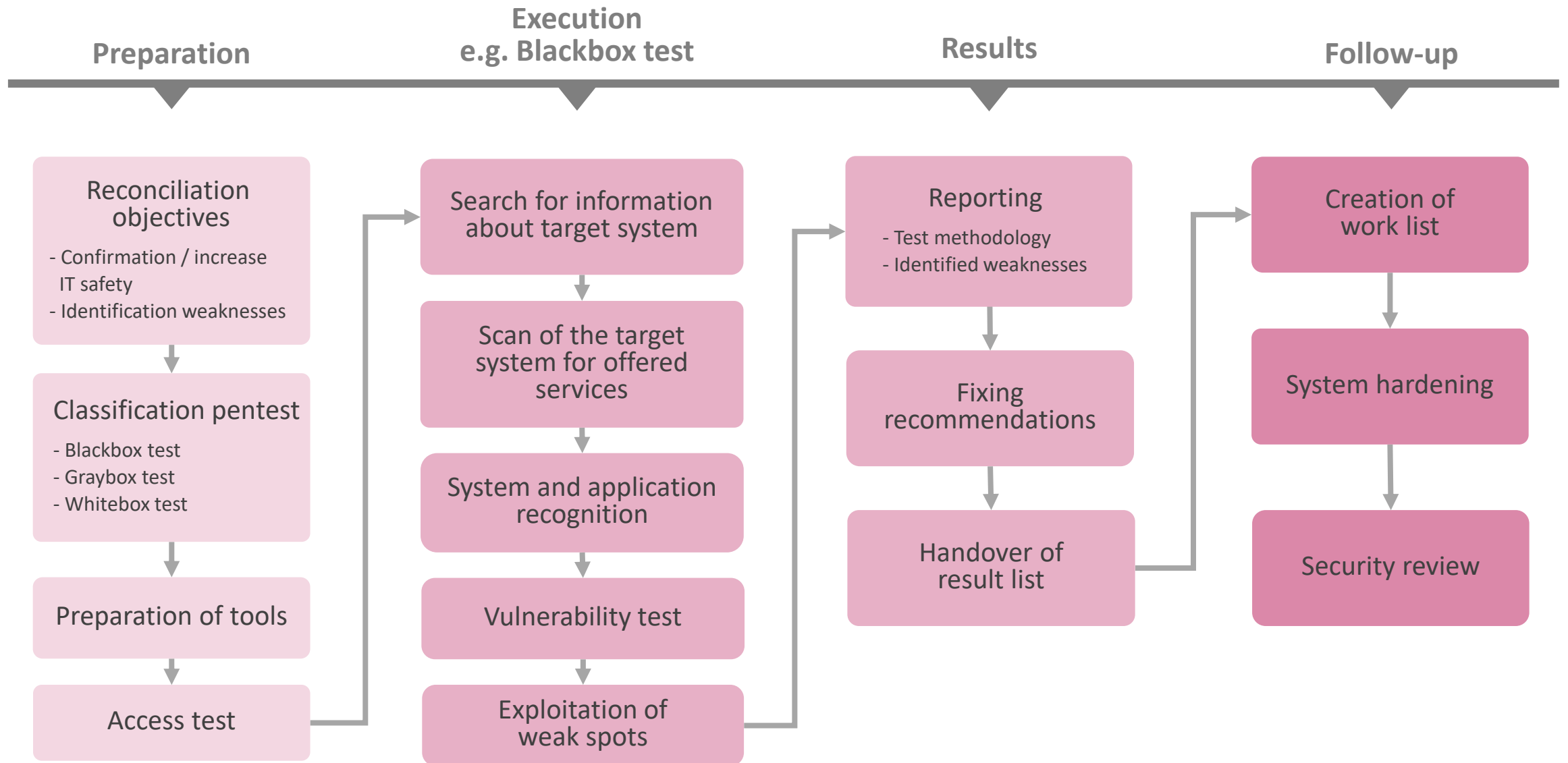
**“With the SAST SUITE, we save around 20 working days for an audit. This hugely relieves the burden on our departments and on IT security.**

**We therefore have greater security and compliance but spend less time to achieve it.”**

**s.Oliver**

**- Matthias Endrich -**

# Procedure of penetration tests:



# 1) Preparation: Classification of pen testing methods

## Criteria:

1. Information base

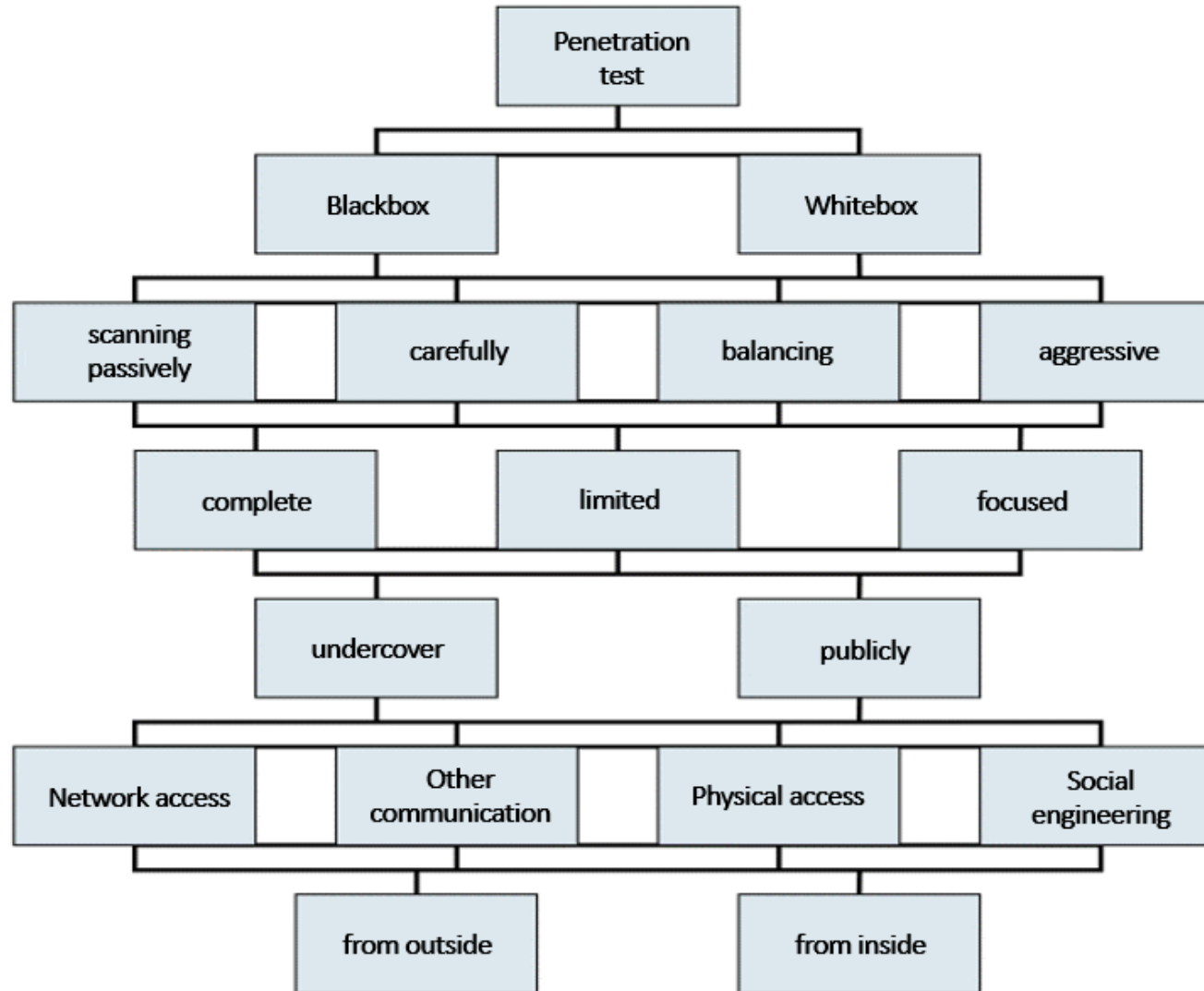
2. Aggressiveness

3. Scope

4. Procedure

5. Technology

6. Starting point



# 1) Preparation: Methods and tools

## ▶ Security / Vulnerability Assessment

- ▶ Components of SAST SUITE

## ▶ IT Security und Compliance Audit

- ▶ Components of SAST SUITE
- ▶ Manual test inside SAP
- ▶ Review of regulations / concepts


## ▶ Penetration test examples

 metasploit® Metasploit: Pen testing framework

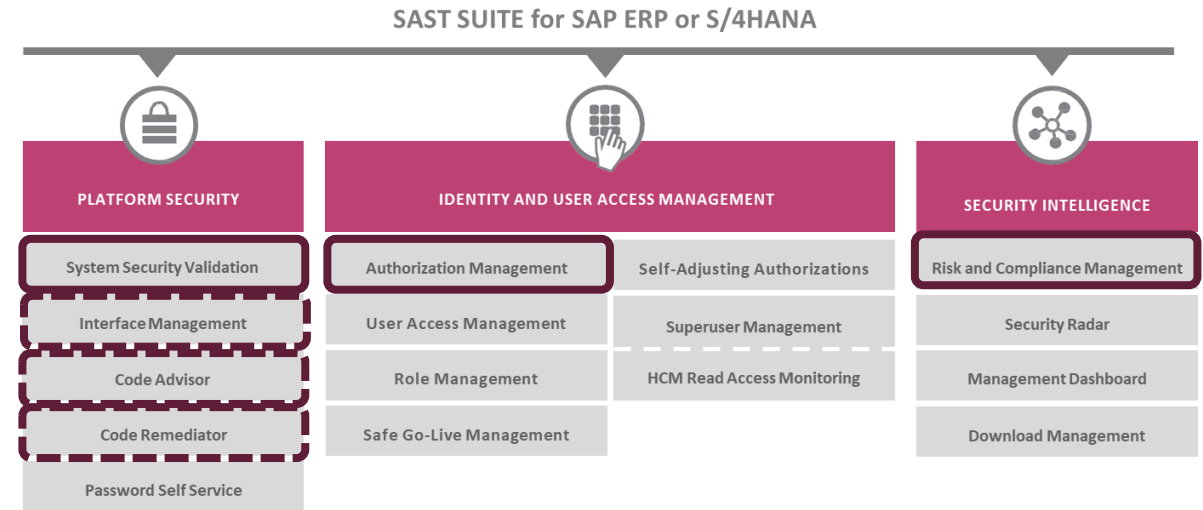
 nessus Professional Nessus: Vulnerability scanner

 NMAP Nmap: Network scanner

 PORTSWIGGER BurpSuite: Pentest / Vulnerability framework

 John the Ripper: Password

 SAST SAST SUITE: Penetration test reports



## 2) Execution: Audit focus and procedure

The audit focus is divided into the following areas:

### Critical authorizations

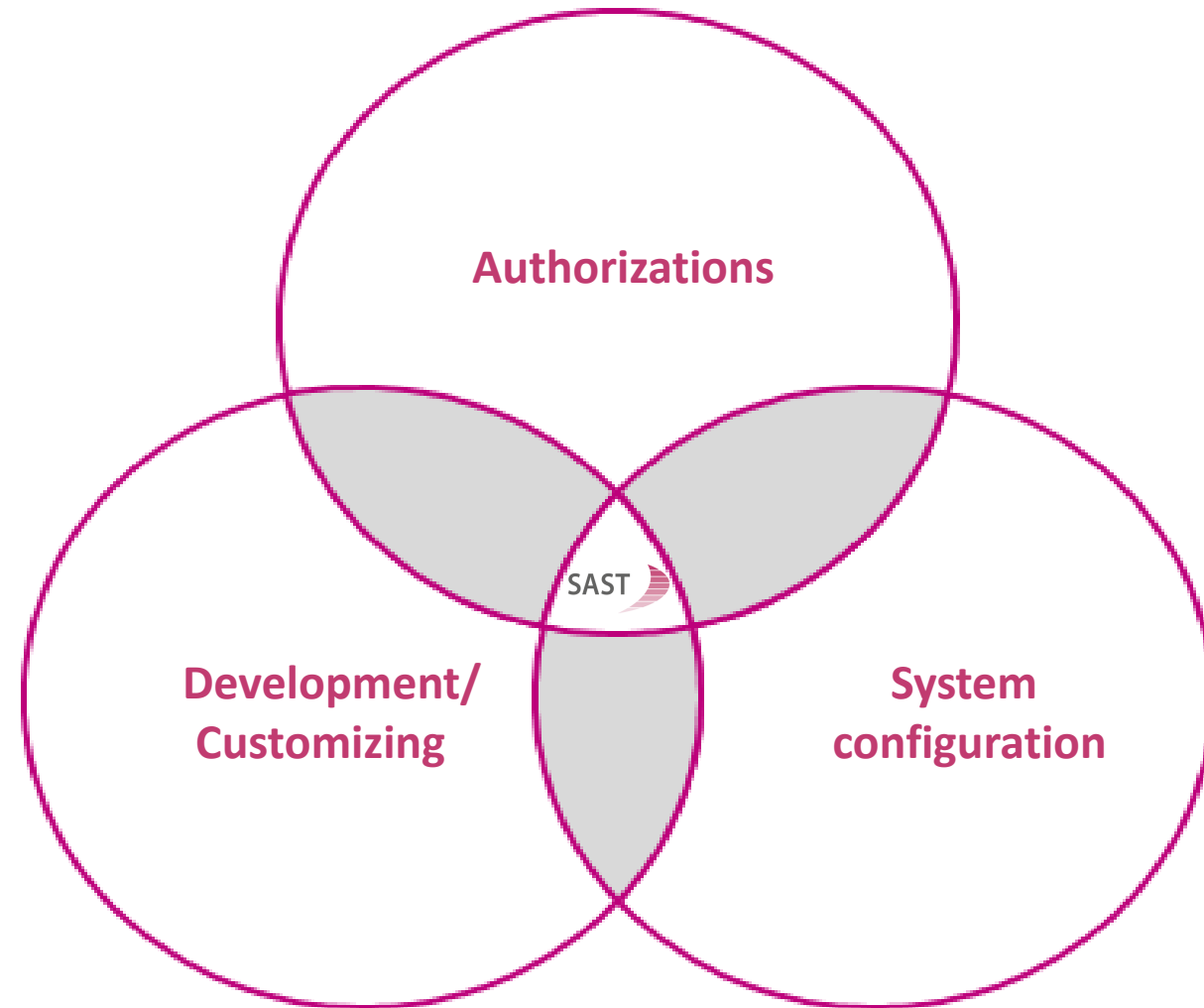
- ▶ Critical profiles and user master data
- ▶ Critical authorizations
- ▶ SoD analysis

### ABAP development and customizing

- ▶ Critical ABAP statements
- ▶ Applications without authorization check
- ▶ Critical authorizations of developers
- ▶ Various customizing settings

### System configuration and operations

- ▶ Operating system and databases
- ▶ Update Status of SAP systems
- ▶ Various security relevant SAP parameters



## 2) Execution: Advantages of SAST SUITE for audit use



### **Comprehensive check of system settings**

- ▶ More than 4.000 checks included in standard delivery
- ▶ Automated validation of security relevant settings and parameters
- ▶ Analyses on all basis platforms
- ▶ Consideration of NetWeaver releases

### **Comprehensive authorization check using certified rule sets**

- ▶ Cross client and cross system authorization check
- ▶ Validation of user master data
- ▶ SoD test for users, profiles and roles in real-time
- ▶ Predefined rule set for SoD violations and confidential access
- ▶ Up-to-date rule framework based on SAP Security Guides, BSI, DSAG Audit Guideline

### **Comparison of the actual values against the current leading practice values**

- ▶ Security Report with clear guidelines for the elimination of vulnerabilities

## 2) Execution: Definition of a testing policy with SAST SUITE

PolicyID	Z_MUSTERKUNDE_AG	Active	Created	SUPPORT	11.05.2020	17:56:34
Description	akquinet Default: SAP Security and Compliance Policy (Version 5.0)			Last updated	SUPPORT	11.05.2020
MatrixID	Z_MUSTERKUNDE_AG					

Node name	CheckID	Description
Operating System		
Unix		
Database		
SAP Hana		
Approach- and access authorities		
Configuration		
Administration of changes of database		
Software scope / timeliness / patch level		
Change Management		
Network		
SAP Systems (Network infrastructure)		
SAProuter		
Configuration		
Change Management		
Approach- and access authorities		
Web Dispatcher / Reverse Proxy		
Service and support connections		
SAP ICM Framework ABAP and JAVA		
SAP Clients		
SAP Application Server (Netweaver)		
SAP System Basis ABAP		
Approach- and access authorities		
Configuration		
ABAP Kernel Parameter		
P_ABAP_001	P_ABAP_001	Parameter: abap/ext_debugging_possible
P_ABAP_175	P_ABAP_175	Parameter: abap/path_normalization
P_ABAP_176	P_ABAP_176	Parameter: abap/dyn_abap_log
P_ABAP_177	P_ABAP_177	Parameter: abap/dyn_abap_log_storage_days
P_ABAP_178	P_ABAP_178	Parameter: abap/dyn_abap_log_deletion_rows
P_ABAP_179	P_ABAP_179	Parameter: abap/authority_to_catch_for_debugging

### Consideration of characteristic system parameters

Header data	
CheckID	P_ABAP_001 Active <input checked="" type="checkbox"/>
Description	Parameter: abap/ext_debugging_possible
Semantics of C	Error if no matches ar... Content component SAP_BASIS
Check Focus	Configuration (System Track)
Check Type	TSE
Manual check	<input type="checkbox"/>
Configurable	<input checked="" type="checkbox"/> Type of configurability SAP Parameter value RZ10
RiskID / Criticality	PARAM00001 / 3 External debugging via RFC/HTTP is possible
ControlID	
Operating system	ANYOS
Database type	DBI
from SAP Release	50A to SAP Release
ABAP or JAVA	ABAP
Output format	Parameter ABAP
Created	SAST-ADMIN 24.02.2014 13:51:25
Last updated	SAST-ADMIN 10.04.2018 11:31:44
Values	
Parameter name	abap/ext_debugging_possible Documentation RZ11
Valid for SAP Release of	50A to
SAP Stack Type	Web AS ABAP
ABAP Stack Parameter	
Operator	Equal to
Value in the production system	2
Depending on	
Parameter name	
Operator	
Value	

Definition of a customer specific testing SAST policy

### 3) Results: Management summary and detailed report

#### System configuration:

Crit.	Risk ID	Description	Parameter	Target value	Actual value
2	PARAM00005	Deactivation of authorization objects allowed	auth/object_disabling_active	N	Y
2	PARAM00008	Tcodes are excluded from authority check	auth/tcodes_not_checked	"SU53 SU56"	undefined
2	PARAM00015	Start of external programs is possible via the gateway.	gw/tcp_security	1	undefined
2	PARAM00093	Security Bypass of ACL files sec_info and reg_info possible	gw/reg_no_conn_info	255	1
2	PARAM00111	XSRF protection: Parameter http/security_session_timeout too high	http/security_session_timeout	900	1800
2	PARAM00086	A user can establish a session via an URL	icf/ssocookie_mandatory	1	0
2	PARAM00076	SAP Internet Framework displays error details.	is/HTTP/show_server_header	FALSE	true
2	PARAM00115	Parameter login/min_password_lowercase too low	login/min_password_lowercase	1	0
2	PARAM00114	Parameter login/min_password_uppercase too low	login/min_password_uppercase	1	0
2	PARAM00112	Potential disclosure of user information	login/show_detailed_errors	0	undefined
2	PARAM00092	System saves backward compatible passwords in table usr02	login/password_downwards_compatibility	0	1
2	PARAM00083	Validity period for unused production passwords too high	login/password_max_idle_productive	0	0
2	PARAM00082	Validity period for unused initial passwords too high	login/password_max_idle_initial	0	0
2	PARAM00080	Enforcement of password policy not activated	login/password_compliance_to_current_policy	1	0
2	PARAM00032	SAP passwords never expire	login/password_expiration_time	0	0
2	PARAM00033	Minimum password length too short	login/min_password_lng	8	6
2	PARAM00057	New password does not have to be sufficiently different from predecessor	login/min_password_diff	3	1
2	PARAM00058	New password must not contain numbers	login/min_password_digits	1	0
2	PARAM00059	New password must not contain letters	login/min_password_letters	2	0
2	PARAM00060	New password must not contain special characters	login/min_password_specials	1	0
Crit.	Risk ID	Description	Parameter	Target value	Actual value
1	PARAM00007	Authority check at CALL SYSTEM deactivated	auth/system_access_check_off	0	undefined
1	PARAM00031	Login with SAP* / PASS would be possible, if user SAP* is missing	login/no_automatic_user_sapstar	1	0
1	PARAM00056	Secure Network Communication not active	snc/enable	1	0
1	PARAM00118	Usage of standard keys for the safe storage	rsec/securestorage/keyfile		undefined

### 3) Results: List of vulnerabilities security / vulnerability assessment

#### Critical authorizations and SoD conflicts:

**Vulnerabilities: Critical authorizations**

Client	Risk ID	Risk Description	Criticality	Total number of user
001	AUTH_00009	Authorization to add and change clients	1	2
001	AUTH_00009	Authorization to add and change clients	1	11
001	AUTH_00200	Authorization to change customizing settings.	1	2
001	AUTH_00125	Authorization to administer the database	1	8
001	AUTH_00180	BC: S_DATASET Write or delete on all files possible	1	123
001	AUTH_00010	Authorization to debug and replace data in productive systems	1	123
001	AUTH_00179	BC: S_DATASET Read access to all files	2	35
001	AUTH_00011	Authorization for developing in productive systems	1	22
001	AUTH_00236	Permission to define external break points	2	11
001	AUTH_00012	Authorization to download files and lists	2	25
001	AUTH_00012	Authorization to download files and lists	2	2
001	AUTH_00171	Permission to perform SAP system measurements		
001	AUTH_00018	Authorization to register as a trusted system / RFC-Administrat		
001	AUTH_00153	Authorization to create and maintain authorization roles (PFCC		

**Vulnerabilities: Segregation of duty**

Client	Risk ID	Risk Description	Criticality	Total number of user
400	SOD_BC_004	Change authorizations & assign authorizations	1	23
001	SOD_BC_005	Authorization administration & user administration	1	445
001	SOD_BC_006	Create BTCL sessions & process BTCL sessions under different userid	1	14
001	SOD_GL_005	FI-GL: Open/close accounting periods / post currency valuation	2	0
001	SOD_BC_003	Function separation: Change the system changeability and workbench maint	1	12
001	SOD_BC_002	Function separation: Change the system changeability and table mainten	1	22
001	SOD_BC_007	Maintain OS commands & Start os Commands	1	98
001	SOD_SAST_1	SAST: Maintenance supportuser SAST & assignment SAP profiles/roles	1	33
001	SOD_GL_001	FI-GL: Change/maintain G/L account in accounting area / account document	2	1
001	SOD_GL_002	FI-GL: Open/close accounting periods / post GL documents	2	77
001	SOD_CO_001	Maintenance cost center & unauthorized costtransfer	3	13
001	SOD_CO_004	Maint cost center grp./cost elementgroup & booking unauthorized revenues	3	54
001	HR_SOD_018	Change HR-payments vs. edit payroll accountings.	2	45
001	HR_SOD_006	Changing the payroll accountings config. vs. deletion billing data 2	2	11
001	HR_SOD_004	Modify the payroll accounting config. vs.maintain the payroll accounting	2	55
001	HR_SOD_014	Edit time data vs. execute time evaluations.	4	8

### 3) Results: Audit report IT security & compliance audit

#### Statistik System AMP (ERP)

Risk of vulnerabilities	Anzahl	Erklärung
Critical	132	Extreme risk, to be principle avoided
High	180	Highly increased risk, without measures not tolerable
Medium	91	Increased risk, temporarily tolerable

#### Statistik System BWP (BI and BO)

Risk of vulnerabilities	Anzahl	Erklärung
Critical	114	Extreme risk, to be principle avoided
High	139	Highly increased risk, without measures not tolerable
Medium	76	Increased risk, temporarily tolerable

#### Statistik System BJP (BI Frontend)

Risk of vulnerabilities	Anzahl	Erklärung
Critical	10	Extreme risk, to be principle avoided
High	30	Highly increased risk, without measures not tolerable
Medium	5	Increased risk, temporarily tolerable

#### Statistik System SSM incl. SAP WebDispatcher and SAP Router

Risk of vulnerabilities	Anzahl	Erklärung
Critical	125	Extreme risk, to be principle avoided
High	149	Highly increased risk, without measures not tolerable
Medium	76	Increased risk, temporarily tolerable

SAST Referenz	Vulnerability	Risk Level
UNIX_00025	File \$HOME/.ssh/authorized_keys not existing or SSH Keys created	1 = Critical
	Through ABAP upload of an AUTHORIZED_KEYS or AUTHORIZED_KEYS2 file into the .ssh directory of the sidadm attacker can gain SSH access to the account of sidadm without password.	
Effort	Recommendation	Effect
Low	Delete the file: \$HOME/.ssh/authorized_keys or \$HOME/.ssh/authorized_keys2  Create a blank file AUTHORIZED_KEYS and AUTHORIZED_KEYS2 Insert an EMPTY file AUTHORIZED_KEYS and AUTHORIZED_KEYS2 in the .ssh directory of SIDADM as a root user. Withdraw the SIDADM write rights to these files to Abstract SIDADM the write permissions on the file to prevent changes, to prevent.	High

SAST Referenz	Vulnerability	Risk Level
UNIX_00016	SSH: Unsecure configuration values (Secure Shell)	2 = High
	The file /etc/ssh/ssh.config contains global configuration values to access Secure Shell. The following values must be set: lenoreRhosts = yes StrictModes = yes RhostsAuthentication = no RhostsRSAAuthentication = no PermitRootLogin = no PermitEmptyPasswords = no Protocol = 2 MaxAuthTries = 5	
Effort	Recommendation	Effect
Low	Change the configuration values in line to your security policy in file /etc/ssh/ssh.config	High

# 3) Results: Testing report

**akquinet**

**Content**

- Restriction of liability ..... 4
- Security and Compliance Test ..... 5
  - Objectives ..... 5
  - Date and time of fieldwork ..... 6
  - Methodic approach ..... 6
  - Applied policies and standards ..... 6
  - System Scope ..... 7
  - Structure of result presentation ..... 7
  - Risk-classification ..... 8
  - Recommendations (Effort and Effect) ..... 9
- Management Summary ..... 10
  - Example: Amount of risks by criticality and area (Technical findings) ..... 12
  - Example: Amount of risks by criticality and area (Authorization related findings) ..... 14
  - Access-authorization SAP Basis & Applications (AL) ..... 14
  - Critical permissions / Criticality 1-3 ..... 14
  - Example list of identified risks (Technical findings) ..... 15
  - Example list of identified risks (Technical findings) ..... 18
- Finding details (Exerpts only) ..... 19
  - AC1 / SAP Applications / Configuration / Configuration SAP FI ..... 19
  - DL1 / Database / Access and Authorizations ..... 20
  - DC1 / Database / Configuration / Protocol files / Audit Logs ..... 21
  - OC2 / Operating System / Configuration / Configuration ..... 21
  - SC1 / SAP System Basis ABAP / Configuration / Proto ..... 21
  - SC10 / SAP System Basis ABAP / Configuration / Gen ..... 21
  - SC13 / SAP System Basis ABAP / Configuration / Stand ..... 21
  - SC14 / SAP System Basis ABAP / Configuration / Gatew ..... 21
  - SC15 / SAP System Basis ABAP / Configuration / Intern ..... 21
  - SC2 / SAP System Basis ABAP / Configuration / Limited ..... 21
  - SC3 / SAP System Basis ABAP / Configuration / Batch ..... 21
  - SC4 / SAP System Basis ABAP / Configuration / OS com ..... 21
  - SC8 / SAP System Basis ABAP / Configuration / Virus pr ..... 21
  - SC9 / SAP System Basis ABAP / Configuration / Other ..... 21
  - SL1 / SAP System Basis ABAP / Logical Access / User ..... 21
  - SL2 / SAP System Basis ABAP / Logical Access / Configu ..... 21
  - SL3 / SAP System Basis ABAP / Logical Access / Trusts ..... 21

**akquinet**

- client change options ..... 30
- report Management System ..... 31
- AP statements in <customer> source code ..... 31
- functions / logging for tables ..... 32
- functions / logging for reports and transactions ..... 32
- ..... 34
- ..... 35
- ..... 43
- ..... 48

Criticality	RiskID	Description
1	ABAP_00002	Critical ABAP statement: DELETE REPORT
1	NW__00011	Active test services for web dynpro ABAP in SICF available
1	ORA_00008	Wrong user in Oracle dba group
2	PARAM00160	Parameter sappgui/nwbc_sripting defined incorrectly
2	PFCG_00002	PFCG: All users can be marked as reference users
2	RFC_00016	Usage of Trusted RFC connections -> Trusted System Information
3	TMS_00008	Test for critical objects during import is deactivated
3	UNIX_00032	Access to FTP Service through <SID>adm possible
3	USER_00006	An unused user-id has been identified

## Segregation of duty conflicts (SOD)

A segregation of duties risk is when a combination of abilities that when assigned to a backend user constitutes a risk. Objective of this risk is to facilitate the appropriate division of responsibilities.

### Example risk:

**Finance:** Maintain Accounting Periods vs. Post Accounting Document in GL Allow a user to inappropriately open accounting periods previously closed and fraudulently post documents to that period after month end. Maintenance of accounting periods should be segregated from the posting of financial transactions in the wrong period.

**Inventory:** The receipt/maintenance of inventory should be segregated from order and invoicing activities.

**Accounts Payable:** Reconciling and releasing blocked vendor invoices should be segregated from daily processing and posting activities.

**Procurement:** Maintenance of contracts and terms should be segregated from payment and billing document changes.

SAST reference	Risk	Risk level
SOD_AUTH_1	SoD Conflicts: Criticality Critical	1 = Critical
	Cumulative RiskID for several single RiskIDs	
Effort	Recommendation	Effect
Low		High

System	Findings
<SID>	For details please test attached XLS file

Description	Amount of user
ABAP development & Export transport & Import transport in PROD	15
AP Payments & Bank Reconciliation	494
AP Payments & Purchase Order Entry	277
AP Payments & Vendor Master Data Maintenance Central	506
AP Voucher Entry & AP Payments	520
AP Voucher Entry & Goods Receipt on PO	1352
AP Voucher Entry & Purchase Order Entry	1088
AP Voucher Entry & Service Receipts Entry	623
AP Voucher Entry & Vendor Master Data Maintenance FI	967

### 3) Results: Presentation of identified weaknesses

#### Management Summary

The examination of the implementation of the external requirements for the content of a proper authorization conception as well as technical system settings and their adherence revealed weaknesses, which in total lead to an operational risk concerning the data confidentiality, integrity and connectivity.



The sum of the findings is in the CRITICAL level. Immediate resolution of criticality 1 vulnerabilities is required / recommended.

The audit involved the production clients. System copies may have inherited the findings on the feeder systems. In particular, vulnerabilities in the basic configuration of the SAP system were identified at the following levels:

- Operating system
- Database
- RFC and gateway
- SAP Basis and Java parameters
- Security patches for SAP software
- Customer programs
- SAP standard user
- SAP dialog user (critical authorizations)

criticality	risik	description
5	very low	No or negligible risk
4	low	Low risk, tolerable without action
3	medium	Increased risk, tolerable for a short time
2	high	High risk, unacceptable without action
1	critical	Extreme risk, to exclude in principle.

Audit area	Criticality			Total Client 100
	Medium Client 100	High Client 100	Very high Client 100	
Operating svstem	0	7	1	8
Database	1	3	2	6
SAP application server	29	78	23	130
Authorizations	81	93	98	272
Concepts/documents	-	6	-	6
<b>Total</b>	<b>111</b>	<b>187</b>	<b>124</b>	<b>422</b>

### 3) Results: Management summary and detailed report

#### ABAP Development:

- ▶ A total of 280 Z programs with at least one critical ABAP statement were identified.
- ▶ A total of 1,500 identified Z programs do not have an authorization check.
  - ▶ About 50% of these have not been changed for at least 10 years.
  - ▶ And about 70% of these have not been changed for at least 5 years.

Critical Statement	Quantity
*CALL* TRANSACTION *	142
*IF*SY-UNAME *	53
*IF*SY-SYSID *	35
*FUNCTION *'SUSR_**	61
*FUNCTION *'BAPI_USER_*	12
*EXEC *SQL*	14
*CALL *FUNCTION *FTP_*	10
*CLIENT* SPECIFIED*	17
*INSERT*REPORT *	1
*DELETE*REPORT *	1

# Average implementation times in comparison:

	Preparation	Execution	Data analysis	Results	Follow-up
	Reconciliation Software Configuration	Tool-added check	Additional test Verification Concepts	Reporting	Presentation Results Recommendation
Sec. Assessment = 4,0 MD	0,5 MD Tool: SAST SUITE	2,0 MD	--	0,5 MD	--
Audit = 8,0 MD	0,5 MD Tool: SAST SUITE	2,0 MD	1,0 MD	4,0 MD	0,5 MD
Penetration test = 5 MD	0,5 – 1,0 MD Tools: Various	3,0 MD	--	1,0 MD	0,5 MD

# 4) Follow-up support: What happens after the security check?

## Creation of work lists

Result: To Do 1 Categorization (according to Eisenhower)

Application Server	
ABAP_00002	Critical ABAP statement: DELETE REPORT
NW_00011	Test services for web dynpro ABAP active
PARAM00055	Secure Network Communication not active

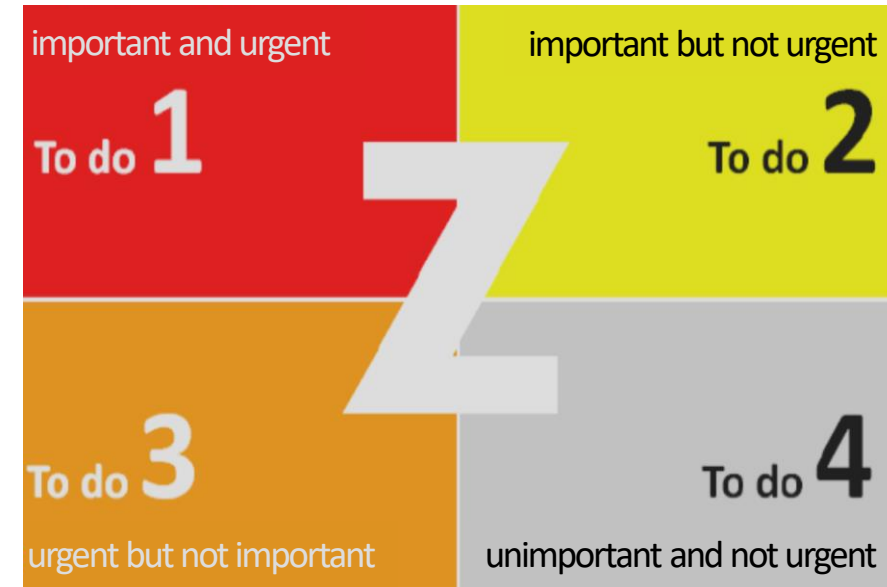
Result: To Do 2 Categorization (according to Eisenhower)

HANA Database	
HANA_00007	Direct assignment system privileges to user master
HANA_00008	Missing encryption of HANA DB volumes
HANA_00010	Privilege "ROLE_ADMIN" has been assigned to normal users
HANA_00015	Parameters: file indexserver.ini - section [repository] - set sqlscript_
HANA_00023	The superuser SYSTEM has not been revoked and replaced by alternative DB

Result: To Do 3 Categorization (according to Eisenhower)

System Settings	
PARAM00079	IGS-Server is administrable via HTTP
PARAM00104	Parameter rdisp/th_popup/strict_check not defined or incorrect
PARAM00129	Parameter rsau/ip_only must be defined on a value of 1
PARAM00150	Parameter gw/rem_start is incorrect
PARAM00153	Parameter: abap/dyn_abap_log defined incorrectly
PARAM00157	Parameters: rsau/log_peer_address logs address incorrectly
PARAM00176	Parameter: dbs/hdb/connect_property incorrect defined
PFCG_00003	PFCG: Object S_RFCACL is generated in the SAP_ALL
PFCG_00004	PFCG: authorization check of Activity 02 is active

## System hardening bases on issue clusters



## Take Home Messages

- ✓ Define in advance, which goal you are pursuing with the building contract.
- ✓ Think about exactly which accents you want to set within the safety analysis (possibly an in-depth interface analysis, code scanning, SoD analysis, etc.).
- ✓ Only then, choose the security service that best suits your situation.  
Let the expert of your confidence support you.
- ✓ If you are already using SAST SUITE, a subsequent "hardening" can be effectively supported by the tool.
- ✓ A tool like SAST SUITE will also provide optimal support for future re-tests and make your tasks considerably easier.

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



TIM KRÄNZKE

Member of the Executive Board

Fon: +49 40 88173-2735

Email: [tim.kraenzke@akquinet.com](mailto:tim.kraenzke@akquinet.com)

Web: [sast-solutions.com](http://sast-solutions.com)