

ACCESS MANAGEMENT

Cybersecurity & Compliance: Secure access according to B3S & NIS2 for KRITIS

Forum A, DE

WALLIX
CYBERSECURITY SIMPLIFIED

WALLIX
CYBERSECURITY SIMPLIFIED



V2.1 - September 2023



Bundesamt
für Sicherheit in der
Informationstechnik



BUSINESS CASES | OPERATIONAL SAVINGS*

AUFWAND
 INITIAL-AUFWAND (STUNDEN):
 FORTLAUFEND (STUNDEN / MONAT):

OHNE PAM	MIT PAM
295	138,5
177	23,15

EINSPARUNG AN ARBEITSAUFWAND DURCH AUTOMATISIERUNG:
 EINSPARUNG AN MANNTAGEN PRO MONAT:

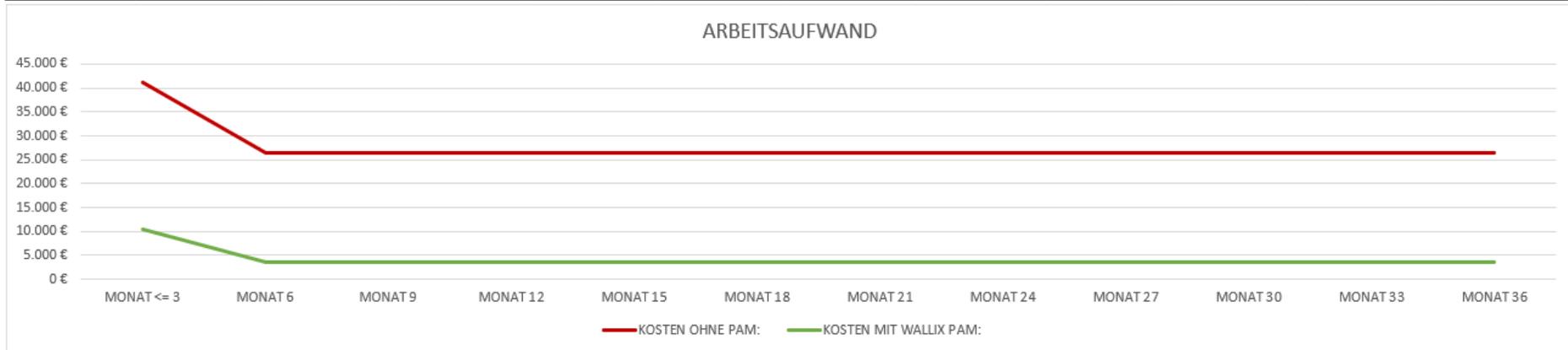
284.755 €
57,69

INITIAL-AUFWAND (KOSTEN):
 FORTLAUFEND (KOSTEN / MONAT):

OHNE PAM	MIT PAM
14.750 €	6.925 €
8.850 €	1.158 €

KOSTEN OHNE PAM:
 KOSTEN MIT WALLIX PAM:

MONAT <= 3	MONAT 6	MONAT 9	MONAT 12	MONAT 15	MONAT 18	MONAT 21	MONAT 24	MONAT 27	MONAT 30	MONAT 33	MONAT 36	GESAMT ÜBER 3 JAHRE
41.300 €	26.550 €	26.550 €	26.550 €	26.550 €	26.550 €	26.550 €	26.550 €	26.550 €	26.550 €	26.550 €	26.550 €	333.350 €
10.398 €	3.473 €	3.473 €	3.473 €	3.473 €	3.473 €	3.473 €	3.473 €	3.473 €	3.473 €	3.473 €	3.473 €	48.595 €



*Scenario: 100 privileged user accounts
 Consistent implementation of ISO27001, Annex A

USE CASE | COMPLIANCE REQUEST



Access **control (access management)** plays a **central role** in all compliance standards, to ensure **data integrity & control structures**

USE CASE | COMPLIANCE REQUEST

Requirements

Personal data must be processed in a manner that ensures adequate security, integrity **and confidentiality** for **them** (GDPR Article 5 ; ISO27001 A.5 - A.18)

Complete personalized traceability and auditability of all data access during a privileged session (GDPR Article 15; ISO27001 A.6, A.9, A.12)

Processors can **only** access **and process** the data **they need** in accordance with applicable security guidelines (GDPR Article 29; ISO27001 A.5,A.9,A.18)

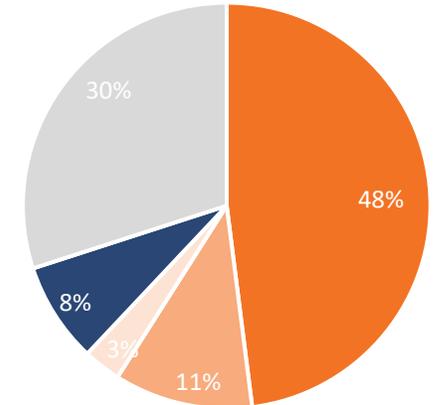
Each controller must keep a **detailed list of all** processing activities in his area of responsibility (GDPR Article 30; ISO27001 A.6,A.9,A.15)

ISO27001, Annex A9

A.9 Access Control

Controls for access control policy, user access management, system and application access control, and user responsibilities

A9.1	Business requirements of access control
A9.1.1	Access control policy
A9.1.2	Access to networks and network services
A9.2	User access management
A9.2.1	User registration and de-registration
A9.2.2	User access provisioning
A9.2.3	Management of privileged access rights
A9.2.4	Management of secret authentication information of users
A9.2.5	Review of user access rights
A9.2.6	Removal or adjustment of access rights
A9.3	User responsibilities
A9.3.1	Use of secret authentication information
A9.4	System and application access control
A9.4.1	Information access restriction
A9.4.2	Secure log-on procedures
A9.4.3	Password management system
A9.4.4	Use of privileged utility programs
A9.4.5	Access control to program source code



- DIRECT MATCH
- PARTIAL MATCH
- INDIRECT MATCH
- MANAGED (ORGANIZATIONAL MEASURES)
- *** NOT APPLICABLE ***

62%

direct and indirect match with ISO27001, Annex A (A5, A6, A7, A8, **A9**, A10, A11, A12, A13, A14, A15, A16, A17, A18)

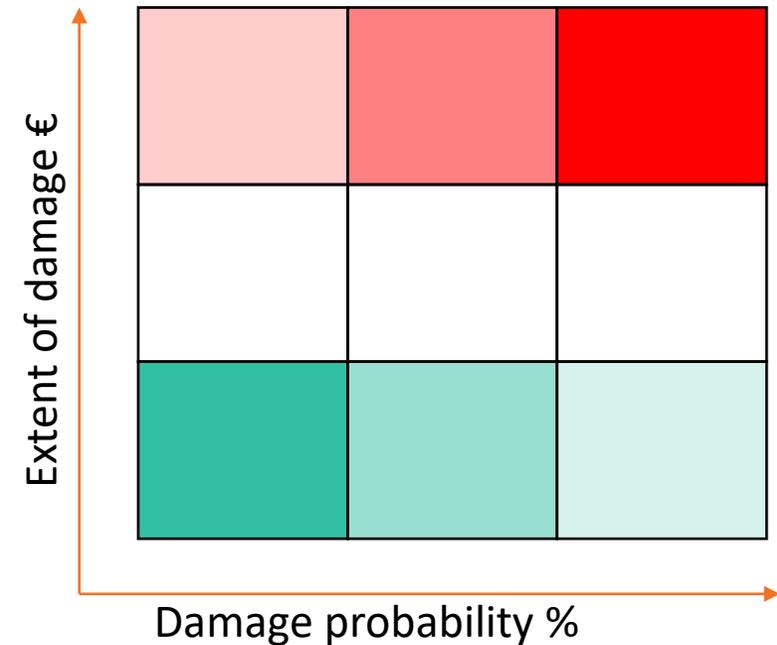
USE CASE | IMPACT ON NON-COMPLIANCE

- **FINANCIAL IMPACT**

- **Security incident costs (e.g. , penalties, damages, ransom, system recovery)**
- **Costs due to operational failures (e.g. , interruption of production and supply chains)**

- **SECURITY RISKS**

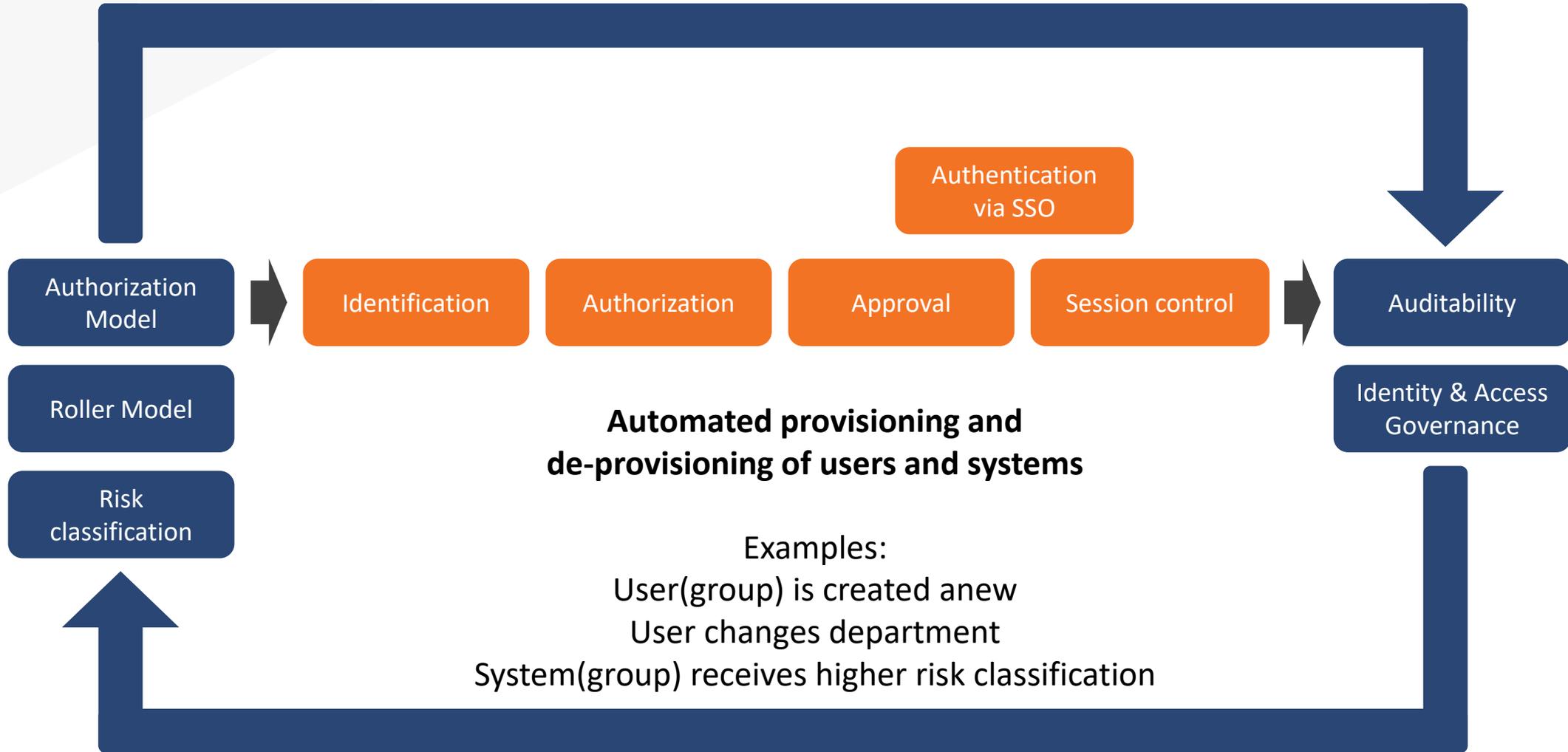
- **Personal injury**
- **Insufficient risk control**
- **No cyber insurance**



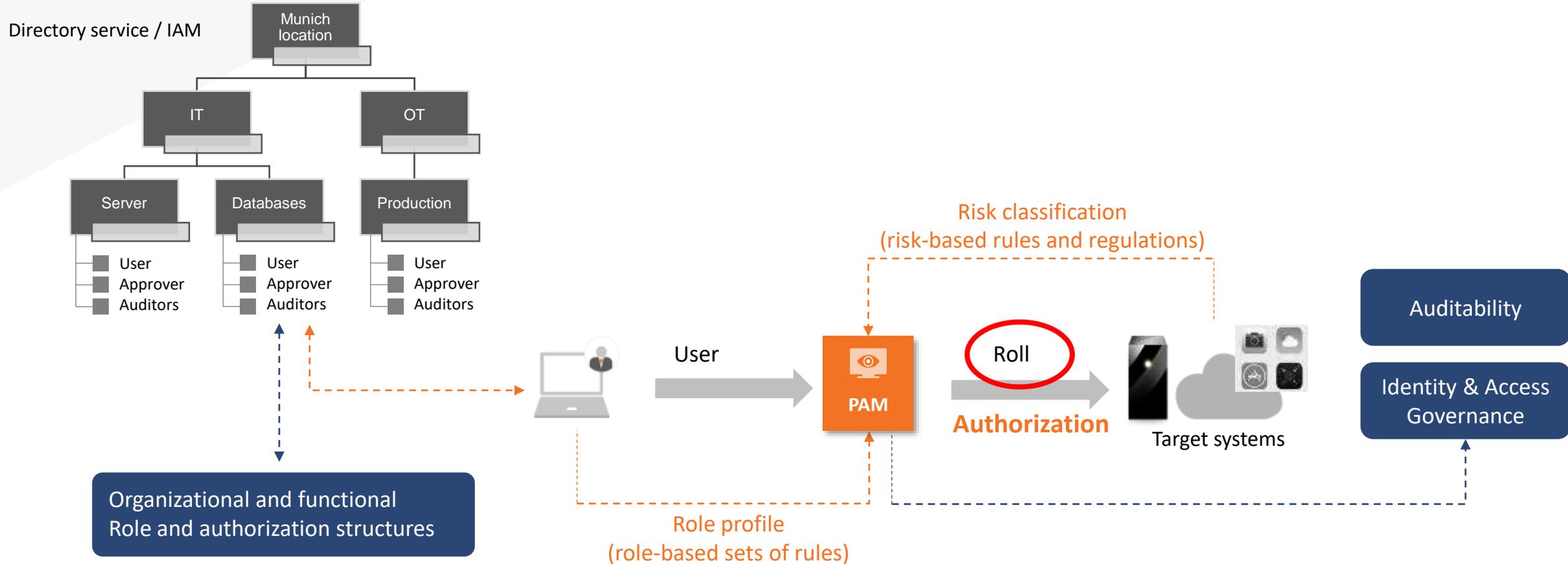
USE CASE | MANUAL VS AUTOMATION

MEASURES BASED ON ISO27001, ANNEX A	MANUAL EFFORT	EFFORT WITH WALLIX PAM
CONCEPTUALIZATION		
Create and manage information security policies (ISO27001, A5)	on a par	on a par
Creating user roles and profiles (ISO27001, A6)	on a par	↑
Definition and management of responsibilities (ISO27001, A7)	on a par	↑
Risk classification of systems (assets) and data (ISO27001, A8)	↑	↑
Creating access concepts (ISO27001, A9)	on a par	↑
OPERATED		
Separation of tasks and roles (segregation of duties) (ISO27001, A6)	on a par	↑
Provisioning and de-provisioning users and permissions (ISO27001, A9)	on a par	↑
Secure authentication procedures (MFA) (ISO27001, A9)	on a par	↑
Use of password management systems for critical assets (ISO27001, A9)	on a par	↑
Implementing key management systems (Key Management) (ISO27001, A10)	on a par	↑
Approval workflows for critical assets (ISO27001, A12)	on a par	↑
Monitor, audit and correlate (privileged) user activities (ISO27001, A12 + A15)	on a par	↑
Monitor and restrict data transfers (ISO27001, A13)	on a par	↑
Traceability and response to security incidents (ISO27001, A16)	on a par	↑
Manage, review and review access permissions (ISO27001, A9 + A15)	on a par	↑
Compliance Reporting (ISO27001, A18)	on a par	↑

USE CASE | AUTOMATED OPERATING MODEL



WALLIX DELIVERIES | BASIC PRINCIPLE



Organizational and functional
Role and authorization structures

NOTE
Pre-made role templates
already available

Authorization = role profile + risk classification

WALLIX DELIVERIES | RISK CLASS MODEL

- **ROLE-BASED ACCOUNT MANAGEMENT** at group level
- **RISK-BASED SYSTEM** management at group level

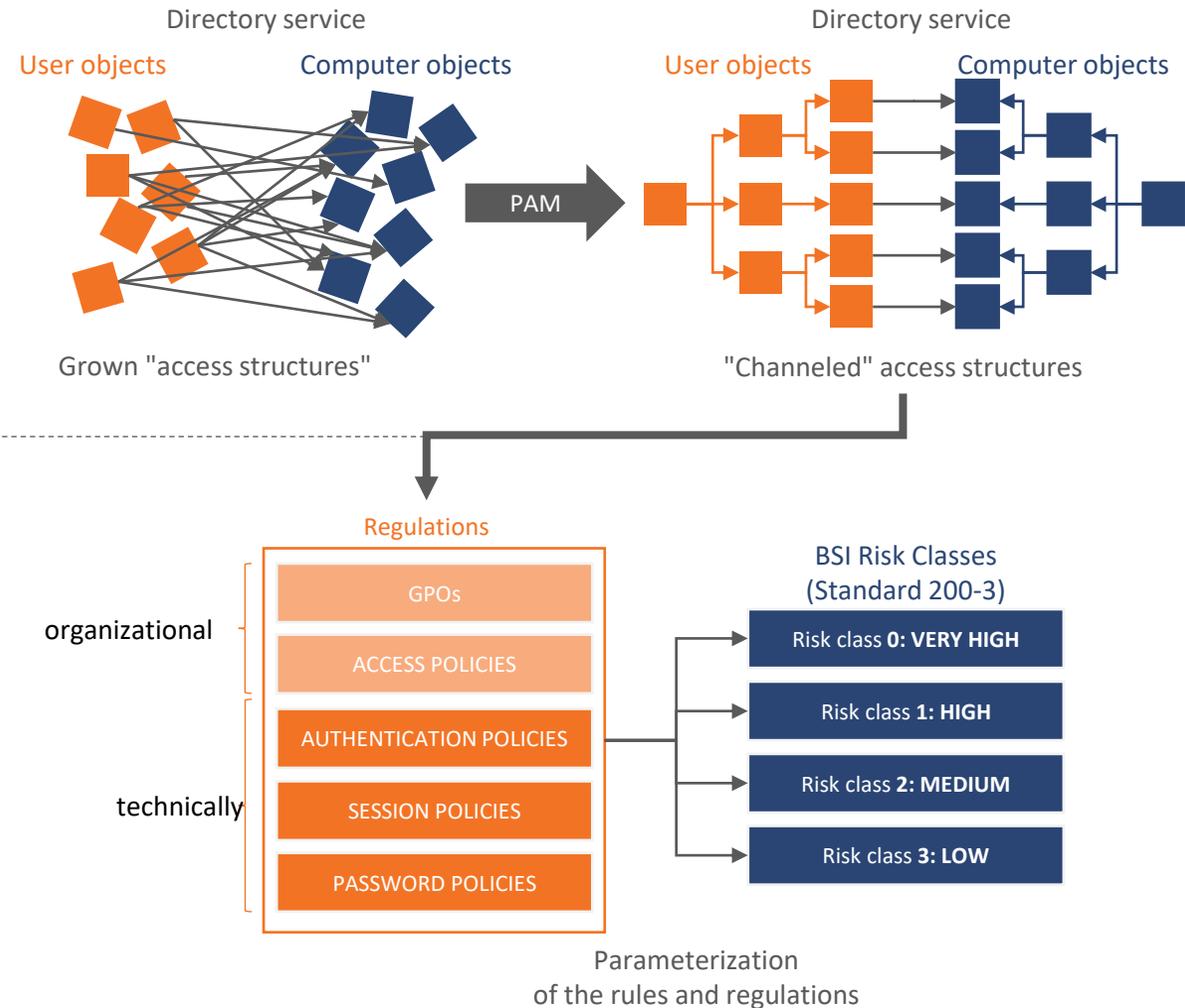
- ➔ **CHANNELED** access via AUTHORIZATIONS
- ➔ **AUTHORIZATION MODEL** via RBAC
- ➔ **MICROSOFT TIERING MODEL** (PAM)

- **TEMPLATES for AUTHORIZATIONS (sets of rules) according to**
 - **BSI-IT Baseline Protection** (BSI Standard 200-3)
 - **ISO27001**, Annex A

➔ IMPLEMENTATION

- Templates with all rules and regulations
- Complete documentation
- Automated commission (Ansible)
- Best Practises: ISO27001, NIST, TISAX, IEC62443

WALLIX RISK CLASS MODEL



WALLIX DELIVERIES | RISK CLASS MODEL

Exemplary rules of the WALLIX risk class model

	VERY HIGH - 0	HIGH - 1	MEDIUM - 2	LOW - 3
AUTHENTICATION POLICIES				
User authentication:	MFA	MFA	MFA*	MFA*
Approval procedure:	required (4 eyes)	required (4 eyes)	required	optional
SESSION POLICIES				
Session recording:	Video + metadata	Video + metadata	Metadata	Metadata
File transfer:	not possible	not possible	about ICAP	about ICAP
Remote connections:	not possible	not possible	restricted	restricted
PASSWORD POLICIES				
Password creation:	by machine	by machine	by machine	by machine
Password change interval:	120 min	weekly	monthly	3-monthly
Password length:	16 characters	12 characters	10 characters	8 characters
Encryption:	4.096 bit, RSA	4.096 bit, RSA	2,048 bits, RSA	2,048 bits, RSA

*: MFA only required outside office hours and from outside the perimeter

WALLIX DELIVERIES | RISK CLASS MODEL

PREVENTION AS AN ESSENTIAL PART OF DIGITAL TRUST

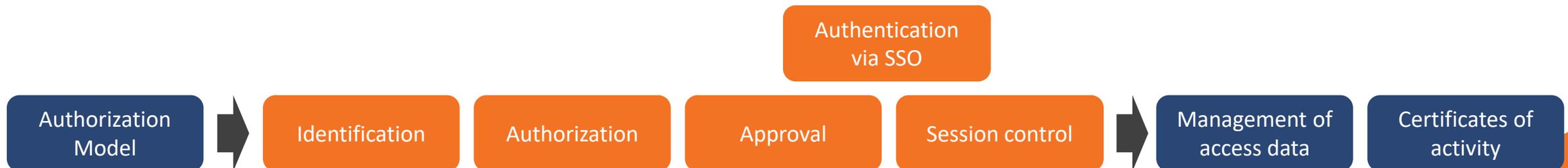
Organizational measures

- List of processing activities
 - Description of user roles, profiles and responsibilities
 - Description and risk classification of critical target systems

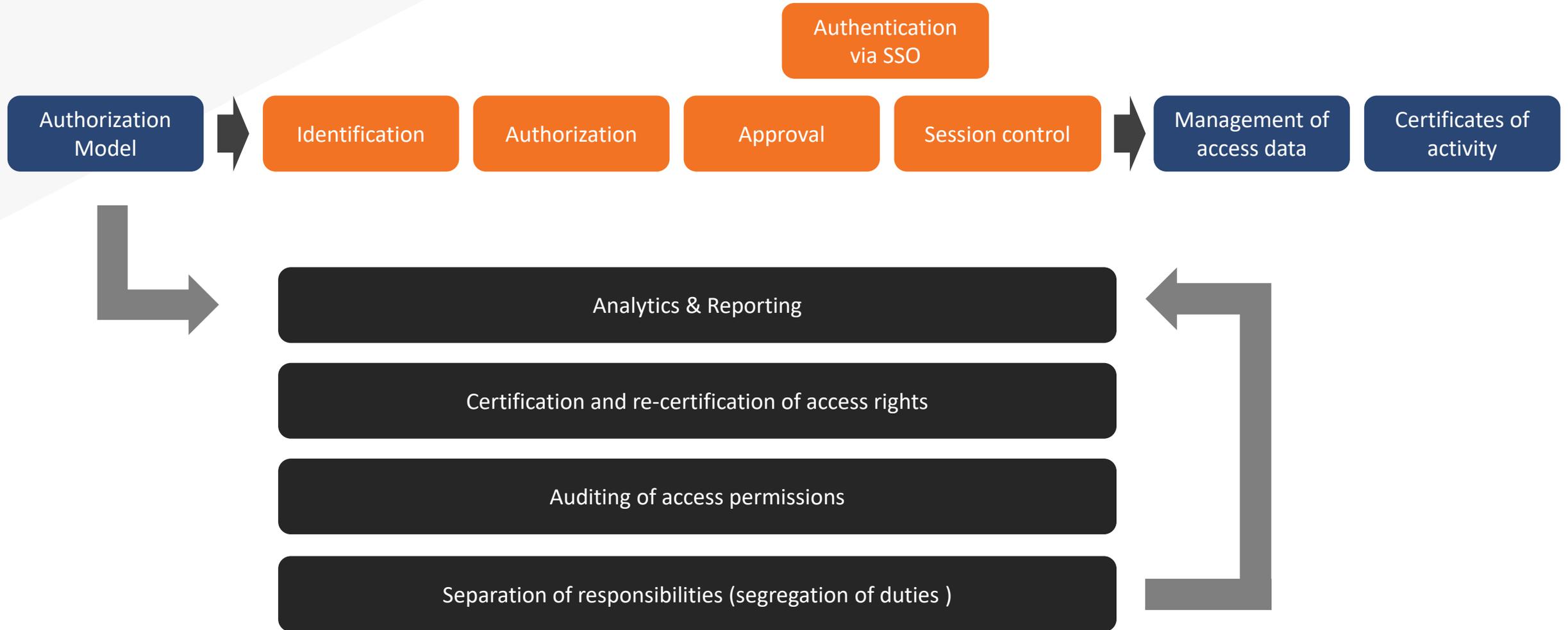
AUTHORIZATION MODEL

Technical measures

- *Identification*: Multi-factor authentication
- *Authorization*: Authorizations according to POLP (Principle of Least Privilege)
- *Approval*: Central approval procedure for critical system access
 - Auditability of approvals
 - Control of access times
- *Session control*:
 - Role-based functional restrictions according to the list of processing activities on system, services, applications and network
 - Comprehensive auditability of currently running sessions (interaction with critical targets)
- *Access data management*: Credential management
- *Activity records*: Complete auditability of processing activities

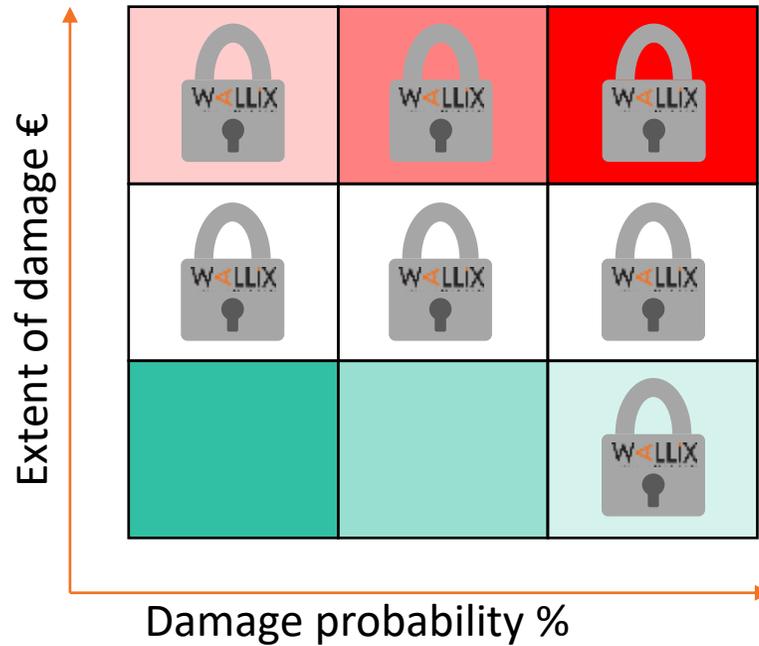


WALLIX DELIVERIES | IDENTITY GOVERNANCE



WALLIX DELIVERIES | RISK CLASS MODEL

- Risk class 0: VERY HIGH
- Risk class 1: HIGH
- Risk class 2: MEDIUM
- Risk class 3: LOW



- ALL privileged access via PAM
Security policies according to risk classes 0 and 1
- ALL privileged access via PAM
Security policies according to risk class 2
- Selected privileged access via PAM
Security policies according to risk class 3

Questions and demos at our booth



WALLIX booth: Hall 6, booth 118

*Whoever controls his access ,
DOMINATES his cyber security.*

*Those who cannot control the access
will NEVER master cyber security!*

Stefan Rabben

Regional Director, DACH

WALLIX GmbH

M: +49 162 283 6973

E: srabben@wallix.com

