IT-SA 2022

Access Management:

Transparenz, Kontrolle und Compliance für KRITIS und Industrie

Stefan Rabben | 26.10.2022

Warum das “Risikoklassenmodell”?

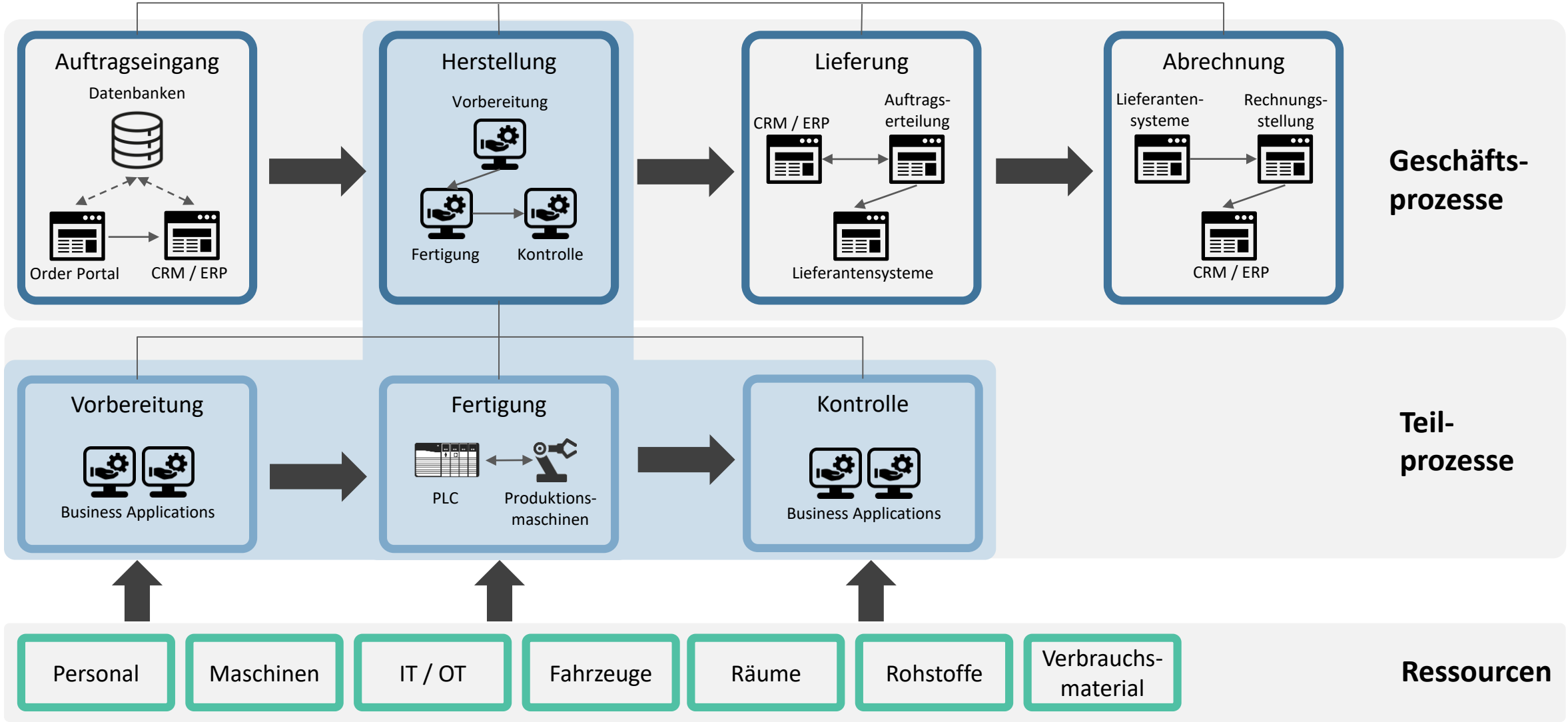
(P)AM Projekte werden verschoben / nicht priorisiert

- Verständnis von Rolle und Bedeutung von Access Management in der Cybersecurity
- Komplexe Anforderungskataloge
- Limitierte Ressourcen in den IT-Abteilungen
- Limitiertes Fachwissen in den IT-Abteilungen

ZIELSETZUNG:

- Schnelle Erklärung der Kritikalität von Access Management in der Cybersecurity
- Schnelle Umsetzung durch Expertenwissen und Standards
- Schnelle Herstellung der **PRODUKTIVITÄT**

Prozesskette



Zielsetzung

Was wollen wir erreichen?

Effiziente Geschäftsprozesse

durch

Maximal mögliche digitale Automatisierung

Optimaler “Total Cost of Ownership” (TCO)

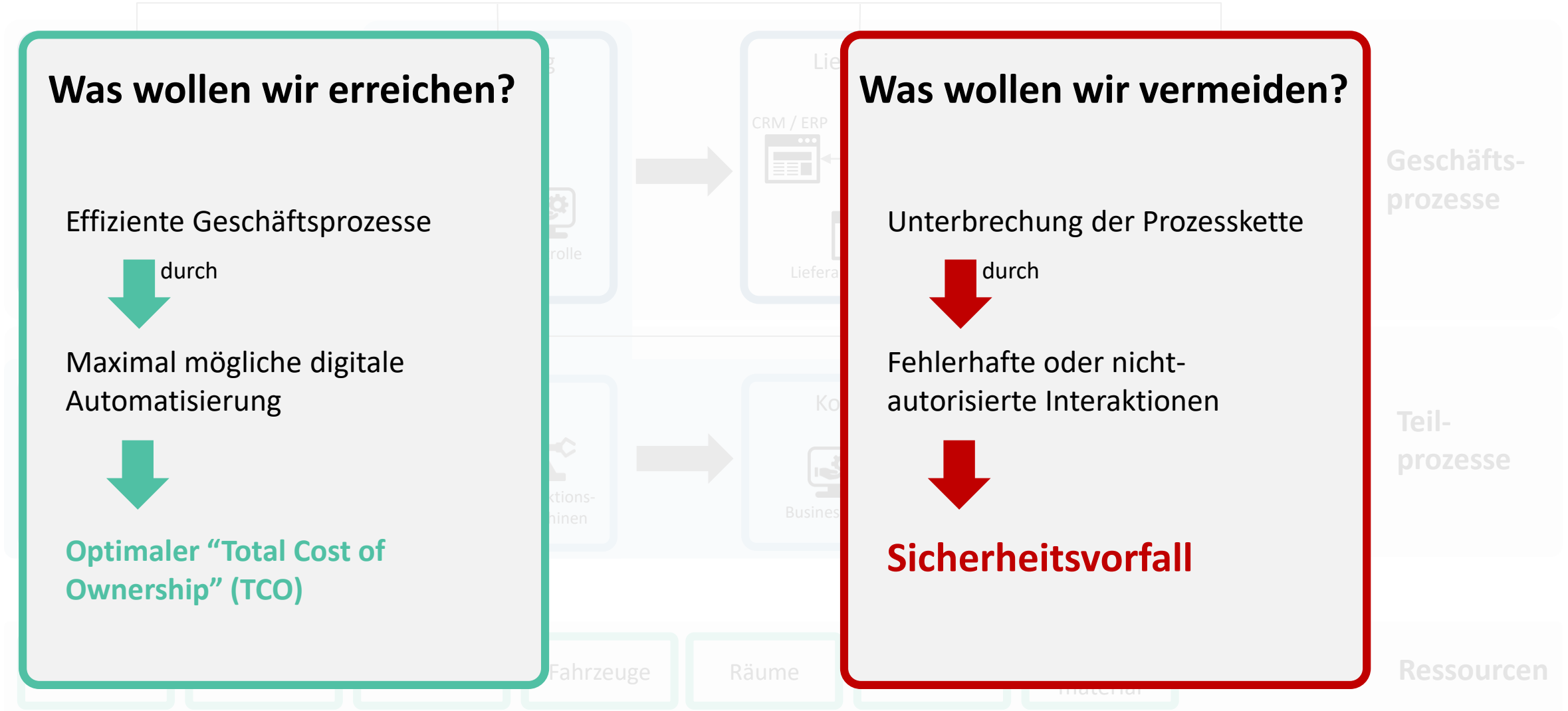
Was wollen wir vermeiden?

Unterbrechung der Prozesskette

durch

Fehlerhafte oder nicht-autorisierte Interaktionen

Sicherheitsvorfall



Zielsetzung

OPTIMALER TOTAL COST OF OWNERSHIP (TCO)

&

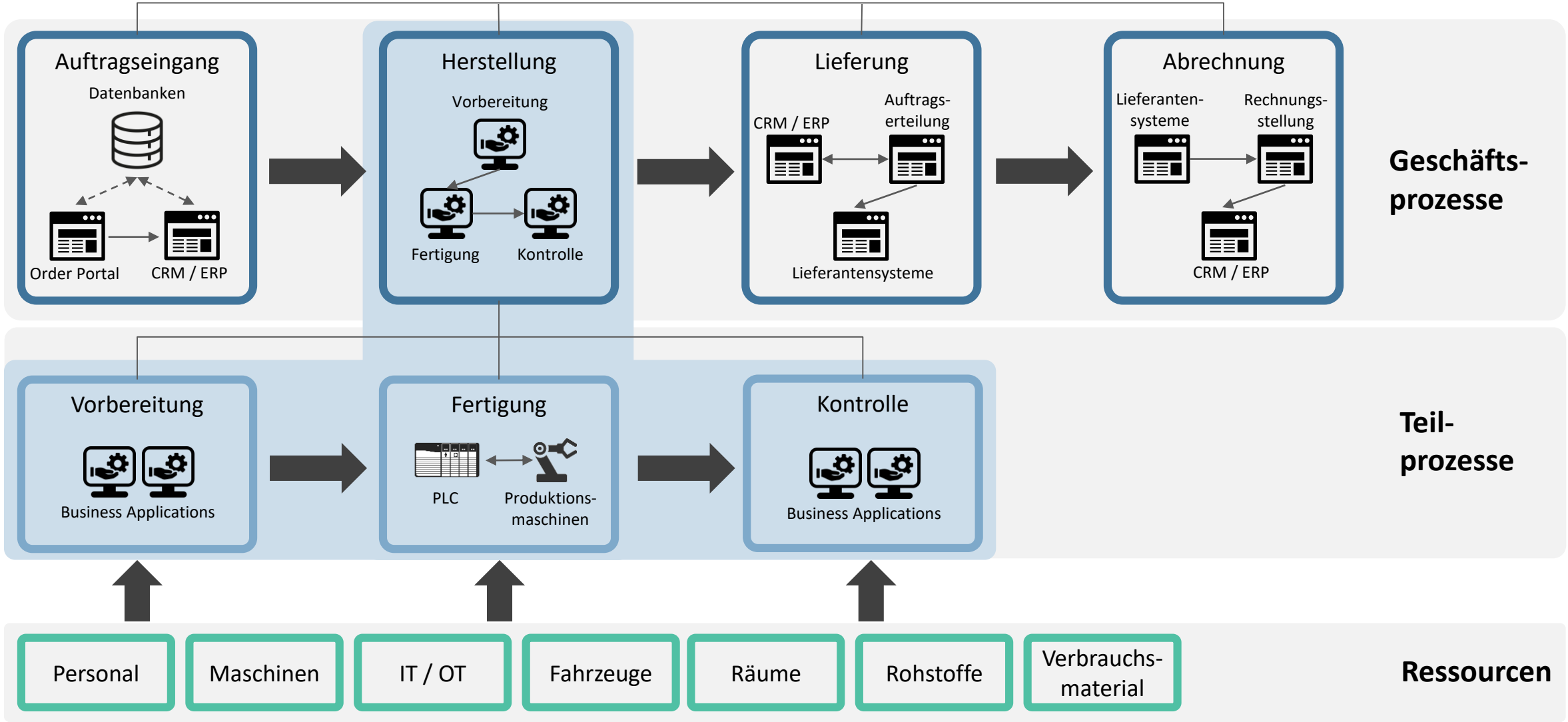
PROFITABILITÄT

CYBERSECURITY

&

RISIKO-MANAGEMENT

Effiziente Geschäftsprozesse



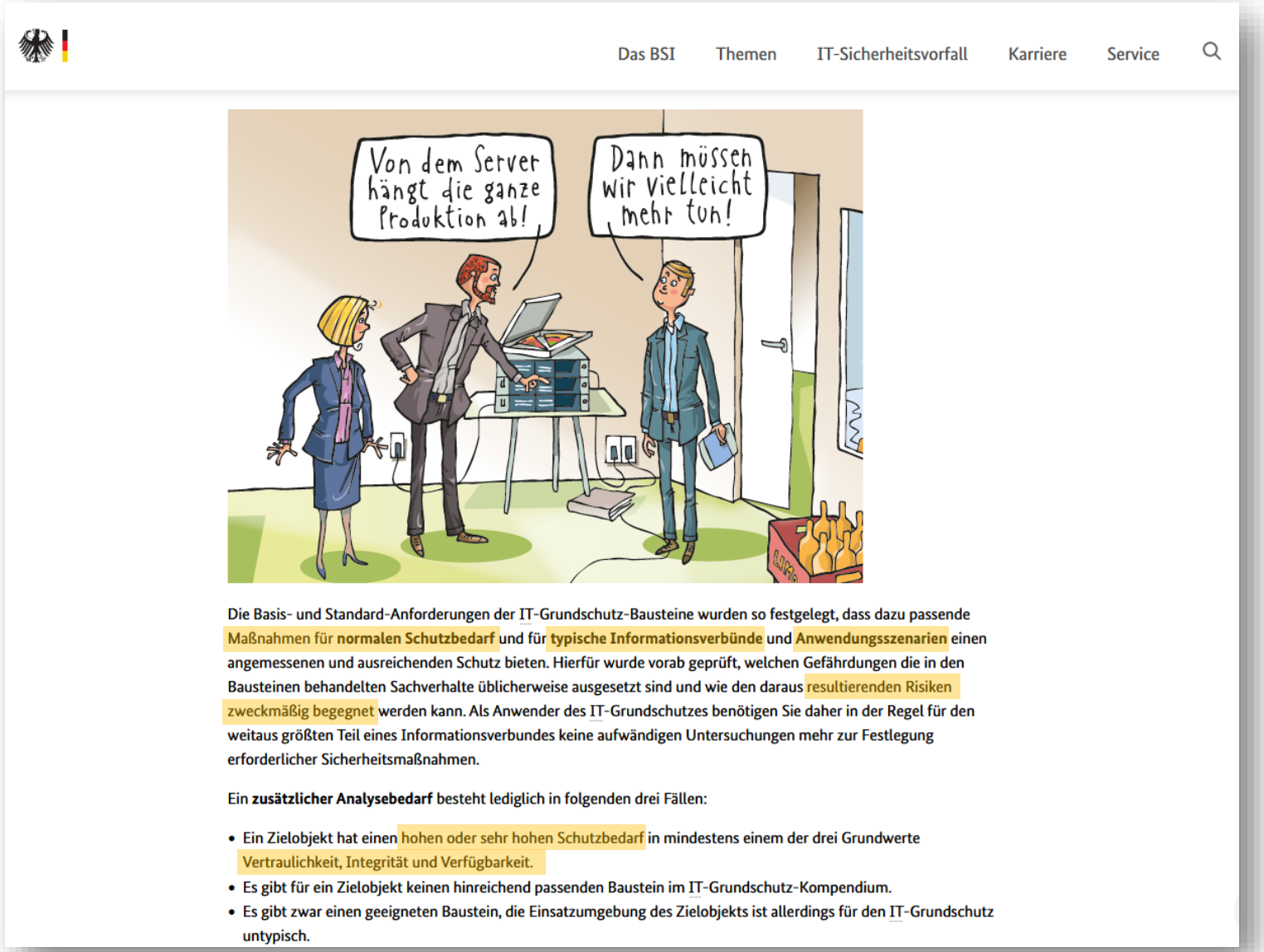
Vermeidung der Unterbrechung der Prozesskette

1. **TRANSPARENZ:**
   Zugriffe und Interaktionen müssen ÜBERWACHT werden

2. **KONTROLLE:**
   Interaktionsregeln gemäß Risikoeinstufung UMGESETZT werden

3. **AUDITIERBARKEIT:**
   Zugriffe und Interaktionen müssen PROTOKOLLIERT werden

Einführung des Risikoklassen-Modells



Das BSI Themen IT-Sicherheitsvorfall Karriere Service

Die Basis- und Standard-Anforderungen der IT-Grundschutz-Bausteine wurden so festgelegt, dass dazu passende Maßnahmen für **normalen Schutzbedarf** und für **typische Informationsverbünde** und **Anwendungsszenarien** einen angemessenen und ausreichenden Schutz bieten. Hierfür wurde vorab geprüft, welchen Gefährdungen die in den Bausteinen behandelten Sachverhalte üblicherweise ausgesetzt sind und wie den daraus resultierenden Risiken zweckmäßig begegnet werden kann. Als Anwender des IT-Grundschutzes benötigen Sie daher in der Regel für den weitaus größten Teil eines Informationsverbundes keine aufwändigen Untersuchungen mehr zur Festlegung erforderlicher Sicherheitsmaßnahmen.

Ein **zusätzlicher Analysebedarf** besteht lediglich in folgenden drei Fällen:

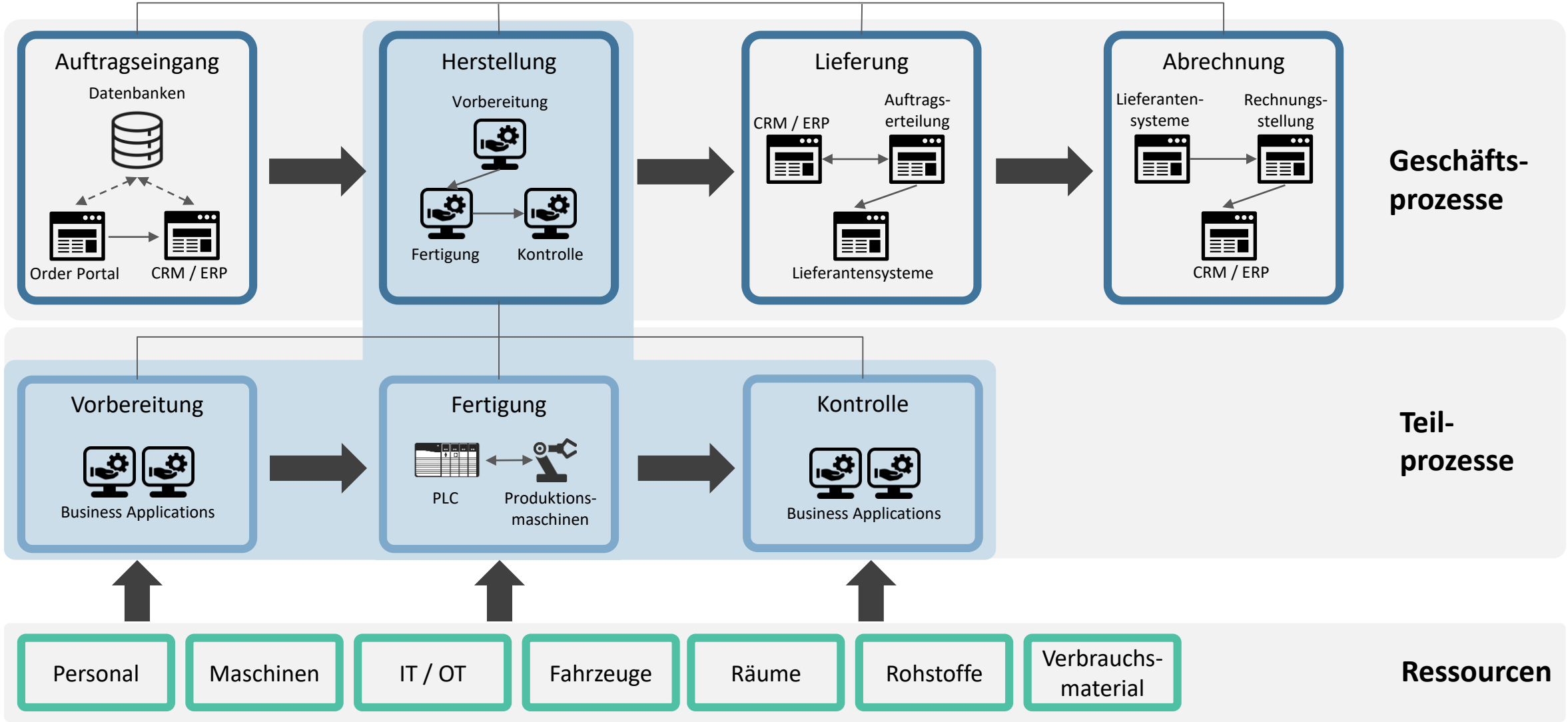
- Ein Zielobjekt hat einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit.
- Es gibt für ein Zielobjekt keinen hinreichend passenden Baustein im IT-Grundschutz-Kompendium.
- Es gibt zwar einen geeigneten Baustein, die Einsatzumgebung des Zielobjekts ist allerdings für den IT-Grundschutz untypisch.

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_7_Risikoanalyse/Lektion_7_node.html

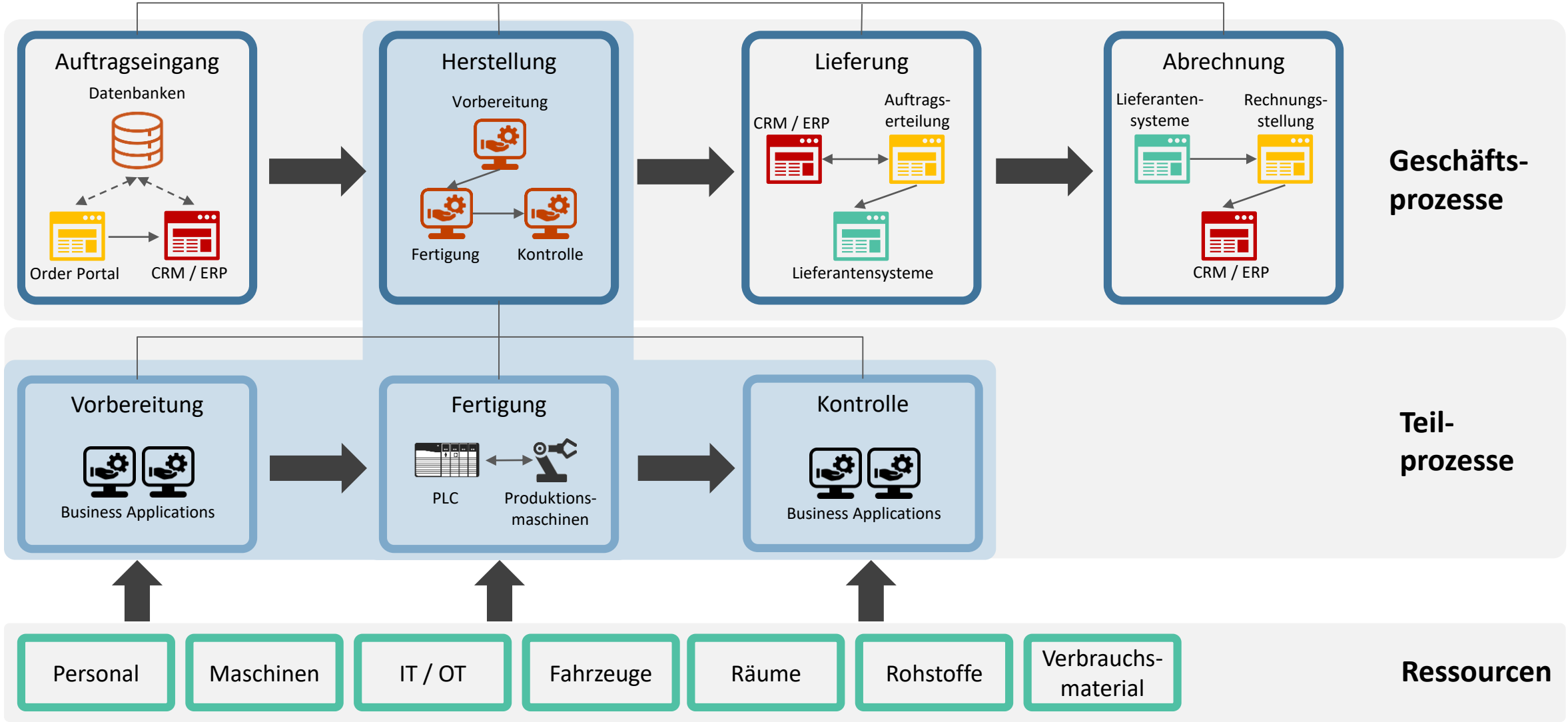
BSI IT-Grundschutz

RISIKOKLASSE 0	**SEHR HOHES RISIKO** Sehr hoher Schutzbedarf
RISIKOKLASSE 1	**HOHES RISIKO** Hoher Schutzbedarf
RISIKOKLASSE 2	**MITTLERES RISIKO** Mittlerer Schutzbedarf
RISIKOKLASSE 3	**NIEDRIGES RISIKO** Niedriger Schutzbedarf

Einstufung nach Risikoklasse



Einstufung nach Risikoklasse



Interaktionsregeln

1. **GRUNDLAGEN:**
   Group Policies (GPOs)

2. **ORGANISATORISCHE MASSNAHMEN:**
   Access Policies

3. **SITZUNGS-KONTROLLE:**
   Authentication Policies | Session Policies | Password Policies

Policies (Regelwerke) durch PAM

Bundesamt für Sicherheit in der Informationstechnik

ISO 27001 International Organization for Standardization

DSGVO KONFORM

Risikoklasse

- DIRECTORY POLICIES (GPOs)
- ACCESS POLICIES
- AUTHENTICATION POLICIES
- SESSION POLICIES
- PASSWORD POLICIES

Parametrisierung

DIRECTORY POLICIES (GROUP POLICY OBJECTSs)
- Definition von PAM als zentrale Zugriffsverwaltung
- Definition der erlaubten Zugriffswege (z.B. Remote Proxy Einstellungen, Clients)
- Erlaubte Zugriffsprotokolle

ACCESS POLICIES (Organisatorische Maßnahmen)
- Welches sind kritische Systeme?
- Wer darf zugreifen (Rollenmodell)?
- Welche Privilegien gelten?
- Von wo und wann darf zugegriffen werden?
- Sind Genehmigungsprozesse notwendig?

AUTHENTICATION POLICIES
- Welche Authentifizierungsverfahren gelten? (z.B. Passwort, SSH-Key, Zertifikat, Kerberos, MFA, …)
- Risikobasierte Verfahren notwendig?

SESSION POLICIES
- Welche Aufgaben dürfen durchgeführt werden?
- Zugriff auf das ganze System oder nur einzelne Applikationen?
- Wird die Sitzung aufgezeichnet?
- Welche zusätzlichen Einschränkungen gibt es? z.B. eingeschränkte Systemdienste wie “MSTSC.exe” oder MMC, ICAP Integration beim File-Transfer, Zwischenablage gesperrt, Remote-Verbindungen möglich, etc.)

PASSWORD POLICIES
- Passwortstärke
- Häufigkeit der Rotation (z.B. alle 30 min oder nach jeder Sitzung)
- Check-in/Check-out Regelwerke
- Notfallmaßnahmen (z.B. Breaking Glass Prozess)

GRUNDLAGEN

ORGANISATORISCHE MASSNAHMEN

SITZUNGSKONTROLLE

Parametrisierung nach Risikoklassen

Parametrisiert nach Risikoklassen (am **BSI IT-Grundschutz**, **ISO27001** und **IEC62443** orientiert)

Automatisches Ausrollen der Regelwerke → ANSIBLE →

Risikoklasse 0 (höchste Priorität) – Linux/SSH Passwort-Richtlinie:

```
Passwortwechselintervall: 60 Minuten
Passwortlänge: mindestens 16 Zeichen
Zeichenaufteilung: mindestens 4 Zeichen jedes Typus
Besonderheiten: keine deutschen Umlaute

Passwortlänge (festgelegt): 16 Zeichen
Sonderzeichen: 4
Kleinbuchstaben: 4
Großbuchstaben: 4
Zahlen: 4

Ausgeschlossene Zeichen: Ä Ö Ü ä ö ü ß

SSH Key Typus: "RSA"
Schlüssellänge: 4096
```

Risikoklasse 1 (hohe Priorität) – Linux/SSH Passwort-Richtlinie:

```
Passwortwechselintervall: Wöchentlich (jeden Sonntag um 12 Uhr)
Passwortlänge: mindestens 12 Zeichen
Zeichenaufteilung: mindestens 2 Zeichen von Großbuchstaben und
Sonderzeichen
Besonderheiten: keine deutschen Umlaute

Passwortlänge (festgelegt): 12 Zeichen
Sonderzeichen: 2
Kleinbuchstaben: 0
Großbuchstaben: 2
Zahlen: 0

Ausgeschlossene Zeichen: Ä Ö Ü ä ö ü ß

SSH Key Typus: "RSA"
Schlüssellänge: 4096
```

Risikoklasse 2 (mittlere Priorität) – Linux/SSH Passwort-Richtlinie:

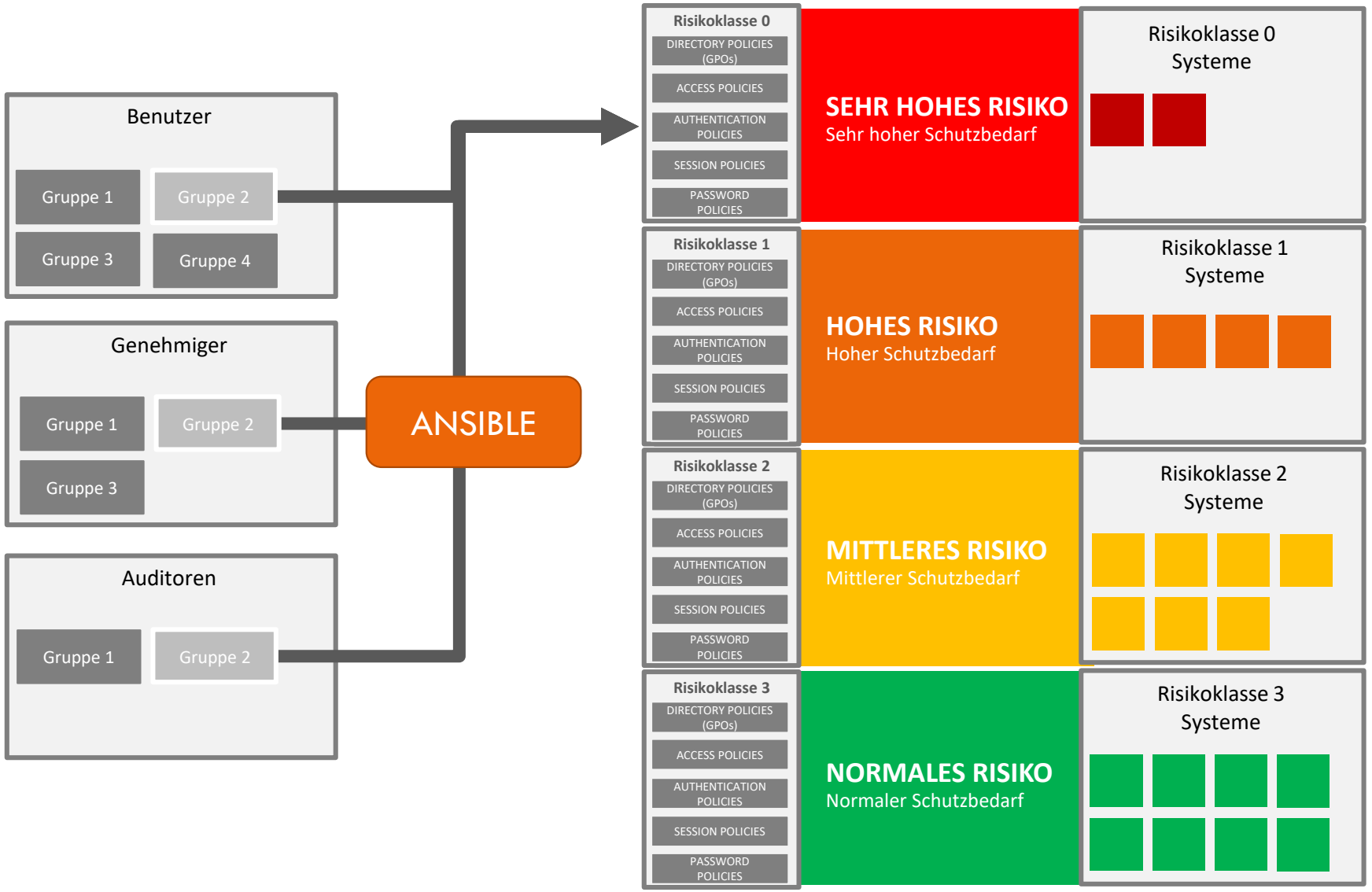
```
Passwortwechselintervall: Monatlich (Erster Tag des Monats)
Passwortlänge: mindestens 10 Zeichen
Zeichenaufteilung: mindestens 1 Zeichen von Großbuchstaben und
Sonderzeichen
Limitierung: keine Limitierungen für Anzahl Groß- und Kleinbuchstaben
Besonderheiten: keine deutschen Umlaute

Passwortlänge (festgelegt): 10 Zeichen
Sonderzeichen: 1
Kleinbuchstaben: 0
Großbuchstaben: 1
Zahlen: 0

Ausgeschlossene Zeichen: Ä Ö Ü ä ö ü ß

SSH Key Typus: "RSA"
Schlüssellänge: 2048
```

Bundesamt für Sicherheit in der Informationstechnik

ISO 27001 International Organization for Standardization

DSGVO KONFORM

Zuordnen der Regelwerke



1. Risikoklassen kritischen Systemen zuordnen
2. Benutzergruppen und -profile aus IAM/LDAP übernehmen
3. Benutzergruppen mit Systemgruppen verbinden

Rollenbasierte Benutzergruppen

Regelwerke (Authorizations)

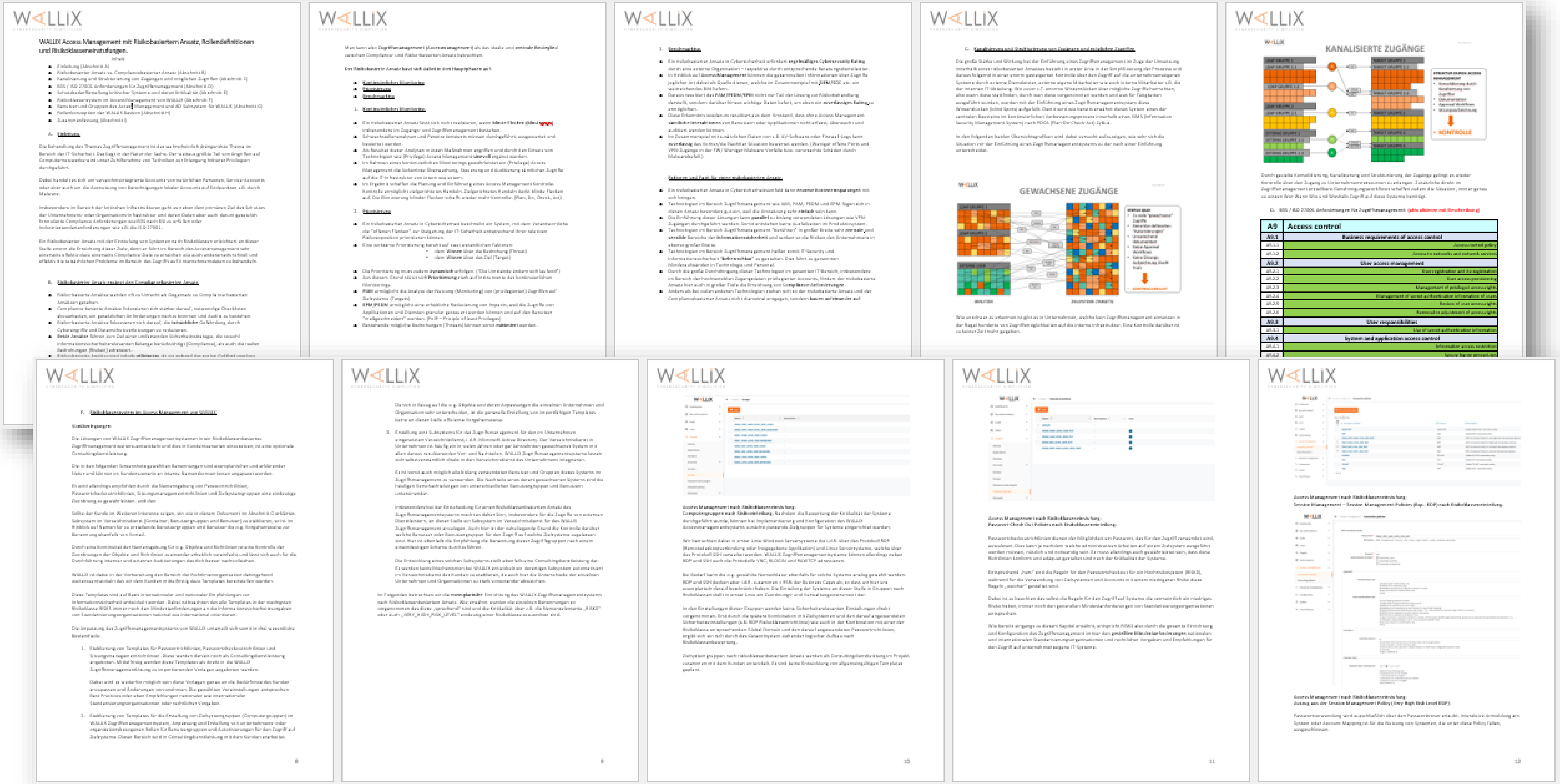
Risikoklassenbasierte Systemgruppen

WALLIX CYBERSECURITY SIMPLIFIED

Dokumentation des Risikoklassen-Modells (Konzept)

www.wallix.com

WALLIX PAM4ALL

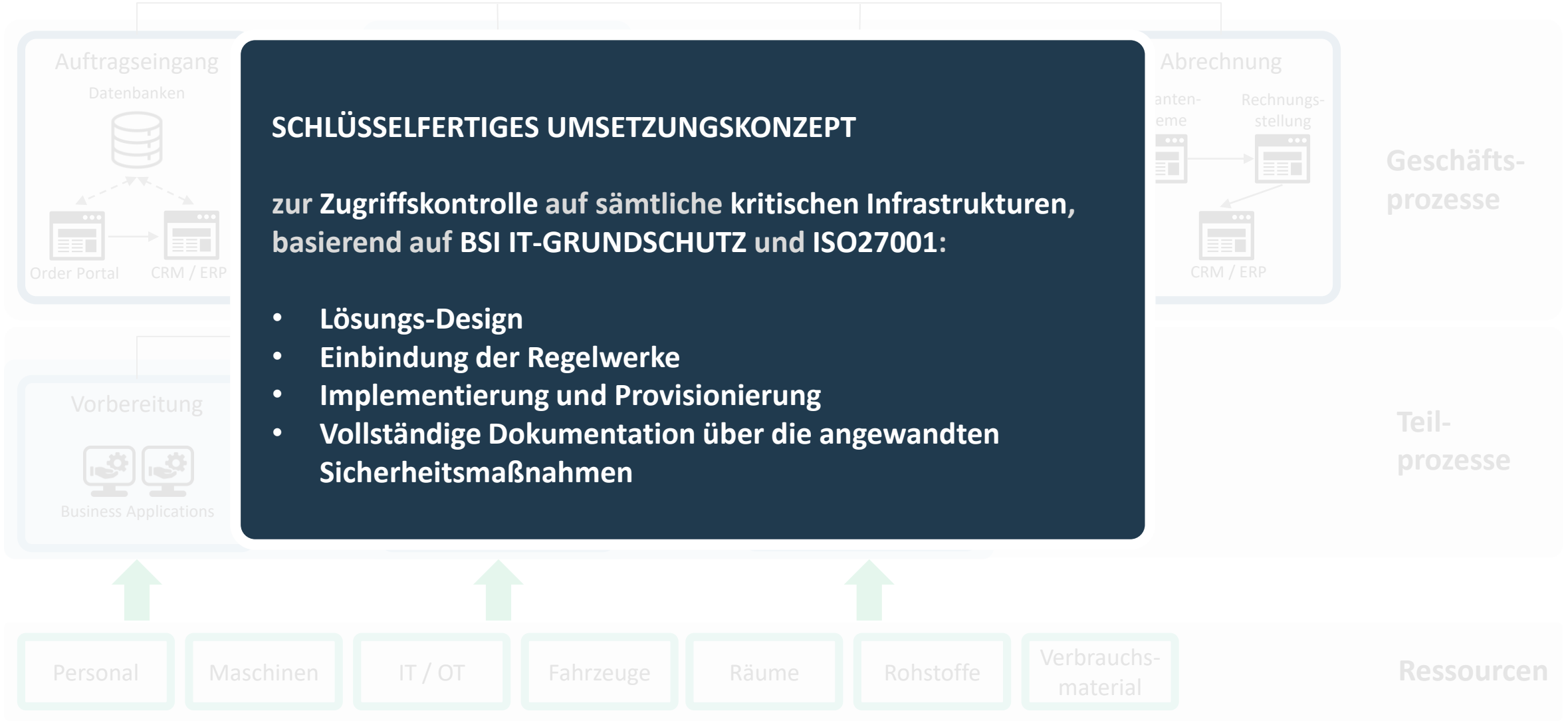


Dokumentation des Risikoklassen-Modells (Regelwerke)

WALLIX Access Management

Risikobasierter Ansatz, Rollendefinitionen und Risikoklasseneinstufungen

Das Ergebnis

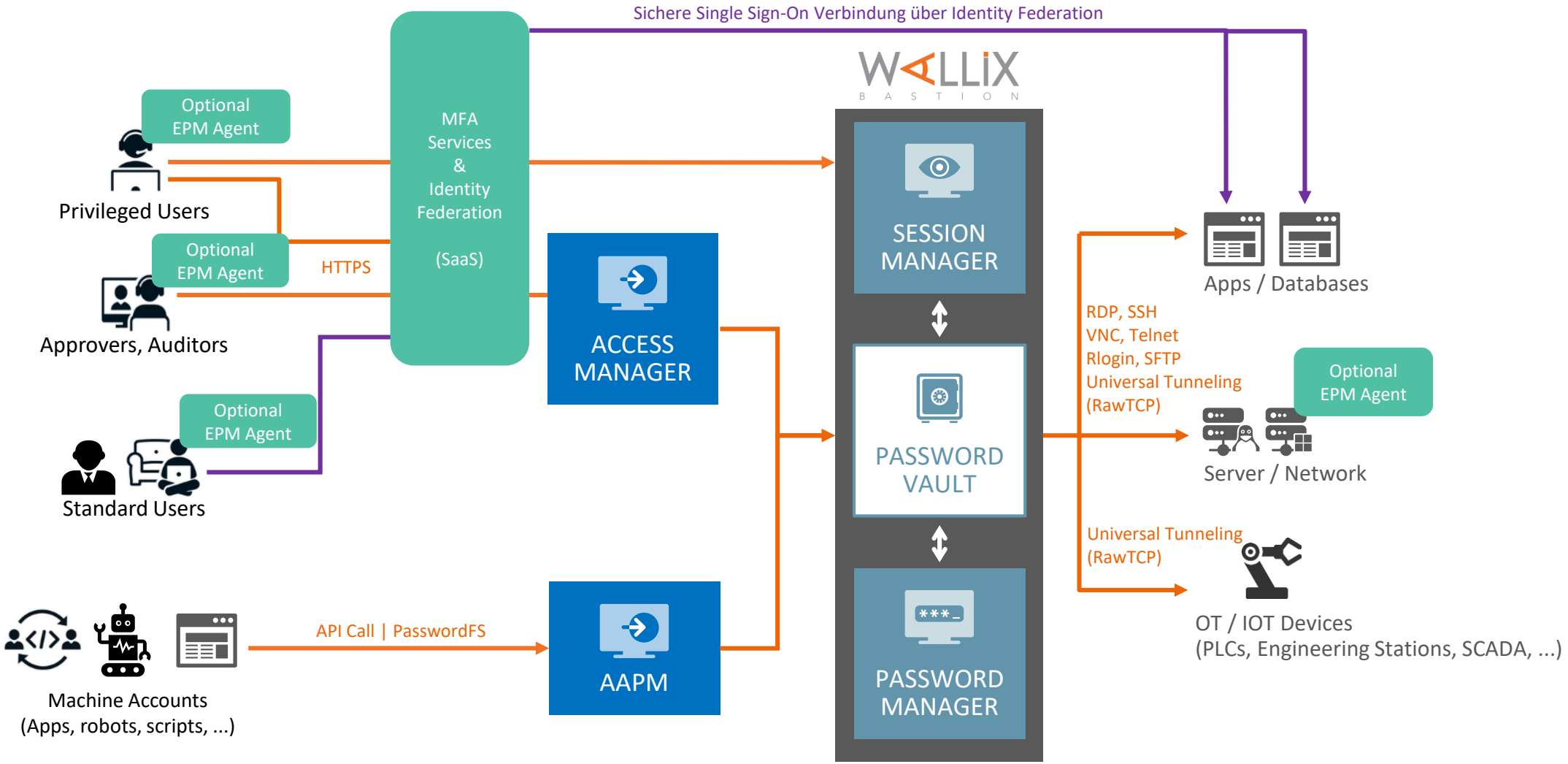


SCHLÜSSELFERTIGES UMSETZUNGSKONZEPT

zur Zugriffskontrolle auf sämtliche kritischen Infrastrukturen, basierend auf BSI IT-GRUNDSCHUTZ und ISO27001:

- **Lösungs-Design**
- **Einbindung der Regelwerke**
- **Implementierung und Provisionierung**
- **Vollständige Dokumentation über die angewandten Sicherheitsmaßnahmen**

Technologie & Architektur



Integrationen

Platforms	Identity IGA/IAM	Multifactor Authentication & SSO	Vault	SIEM	Vulnerability Mgt	DevOps	Antivirus / DLP	ITSM	Other	OT	Behavior Analytics
Microsoft Azure	OGiTiX	gemalto, RSA READY	HashiCorp	LOGPOINT	Qualys.	ANSIBLE	FORCEPOINT	servicenow	Alleantia	fives	CYBER
amazon web services	Evidian	onelogin	HID	CYBERARK	IBM Security	Cyberwatch	Terraform	kaspersky	ConnectWise	bertin	
Google Cloud Platform	SailPoint	inwebo	okta	thycotic	splunk>	tenable	kubernetes	falcongaze	bmc	NUTANIX	
openstack	okta	Ping Identity	DUO		BACKBOX	docker	McAfee				
Microsoft Hyper-v	Brainwave GRC	SecurEnvoy	yubico		blueprism						
vmware READY	Kleverware				beyond SECURITY						
	Azure Active Directory										

Standard Protocols

REST-API

Active Directory

SAML v2.0

SCIM

ICAP

Radius

LDAP.com Lightweight Directory Access Protocol

syslog

KERBEROS

WALLIX PAM4ALL

Die Einführung von PRIVILEGED ACCESS MANAGEMENT ist das BINDEGLIED zwischen den meisten technischen Controls im Anhang A der ISO 27001 zu allen anderen technischen Lösungen im Cybersicherheitsspektrum.

Fragen und Demos bei uns am Stand

Digital Trust:
Virtueller Fallschirmsprung am Stand

WALLIX Stand: Halle 6, Stand 322

Vielen Dank

Stefan Rabben
M: 0162 – 283 6973
E: srabben@wallix.com