

# Informationssicherheit an der FAU nach BSI

https://www.intern.fau.de/informationstechnik-it/infosec/

## < Informationstechnik (IT) und -sicherheit

Gremien und CIO-Office

Anträge an das CIO-Gremium

### Sicherheit

Awareness

E-Mail Zertifikate

Richt- und Leitlinien

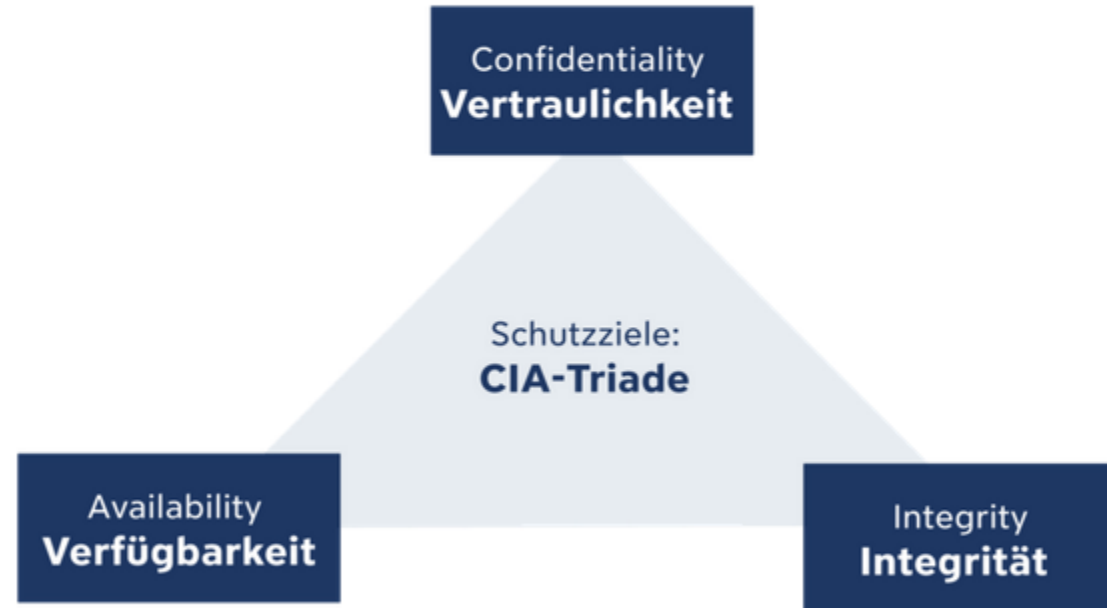
Cyber-Notfall

### Richtlinien

Digitale Barrierefreiheit

IT-Tipps aus dem CIO-Office

## Informationssicherheit und Schutzziele



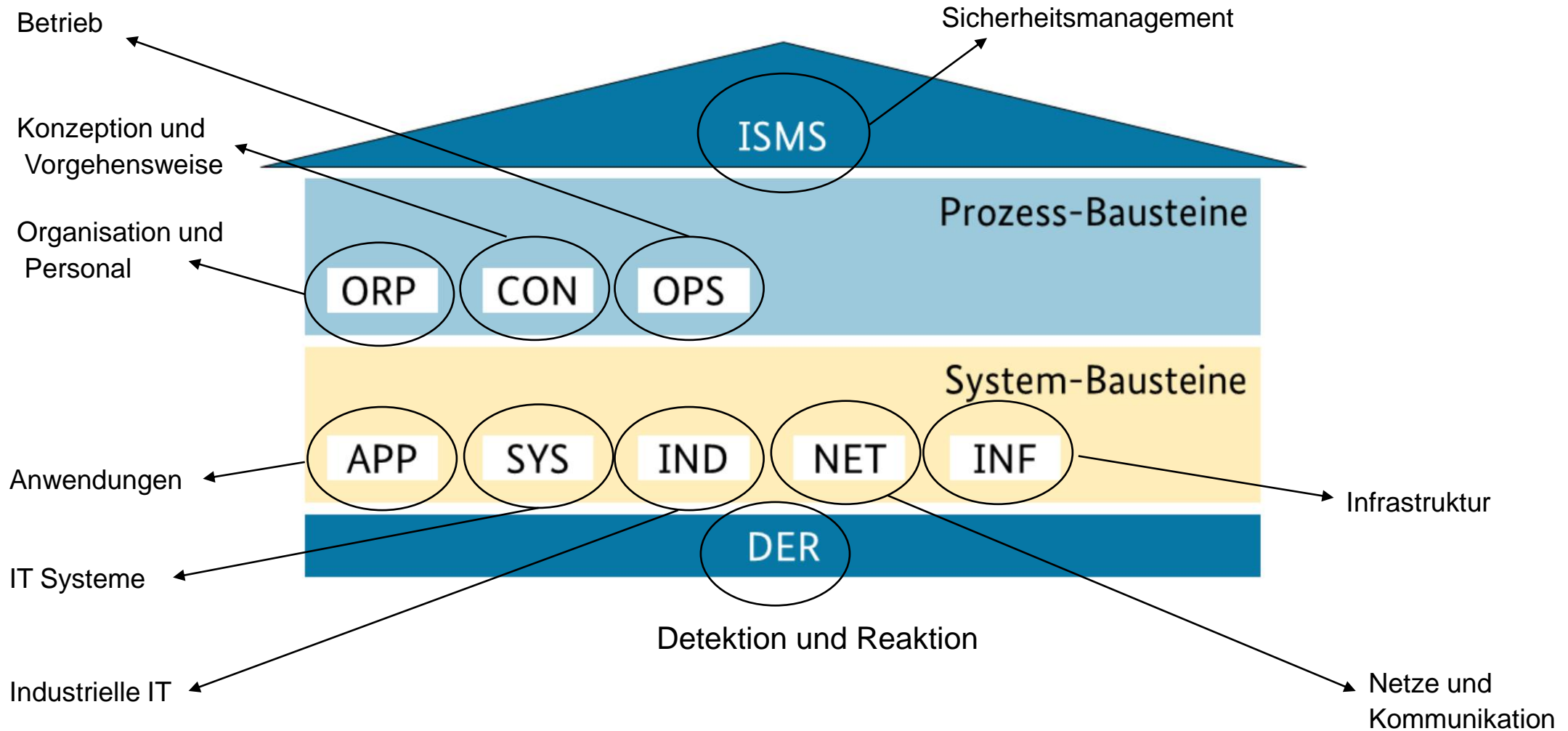
Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability) als Schutzziele der Informationssicherheit.

## ISO/IEC-2700x-Reihe (international)

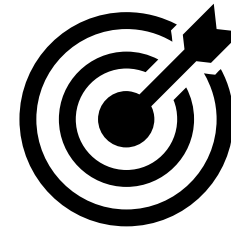
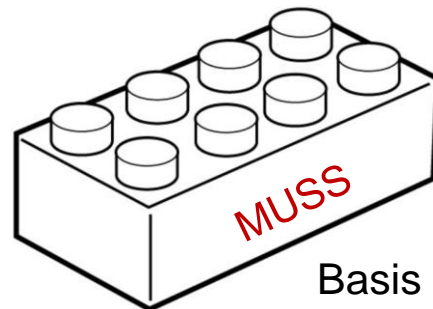
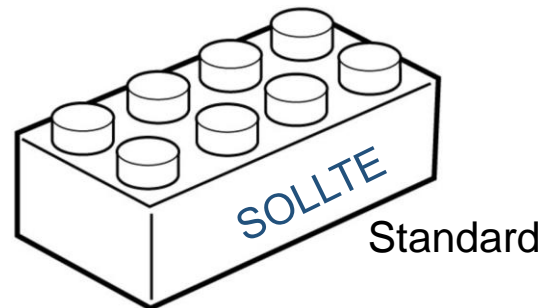
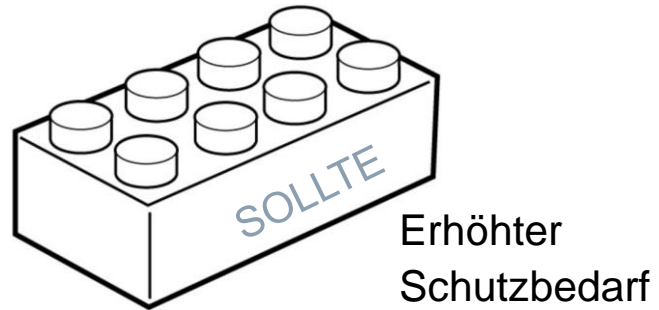
- Insbesondere: 27001, 27002, 27005

## Das BSI liefert 3 Kernaspekte des IT-Grundschutzes:

- IT-Grundschutz **Kompendium**: Fokus auf IT-Grundschutzbausteine
  - Beschreibt u.a. Gefährdungen und Sicherheitsanforderungen
- IT-Grundschutz **Standards**: Vorgehensweisen
  - Beschreiben den Ablauf des Prozesses
- IT-Grundschutz **Profile**: Mustervorlagen
  - Liefern sog. Blaupausen für typische Anwendungsfälle



### Priorität und Bearbeitungsreihenfolge



Ziel

R1

R2

R3



## DER.1 Detektion von sicherheitsrelevanten Ereignissen

R1



*Ein systematischer Weg, wie Informationen **gesammelt, korreliert und ausgewertet** werden können, um sicherheitsrelevante Ereignisse möglichst vollständig und zeitnah zu **detektieren**.*

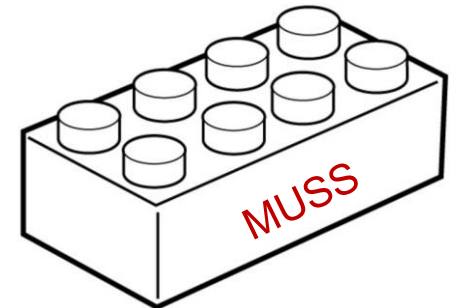


### Gefährdungslage

- Missachtung von gesetzlichen **Vorschriften** und betrieblichen Mitbestimmungsrechten
  - z.B. Sammlung und Auswertung von personenbezogener Informationen
- Unzureichende **Qualifikation** der Mitarbeitenden
  - z.B. nicht ausreichend geschult und sensibilisiert
- Fehlerhafte **Administration** der eingesetzten Detektionssysteme
  - z.B. vermehrte Fehlalarme
- Fehlende **Informationen** über den zu schützenden Informationsverbund
  - z.B. nicht alle Bereiche werden durch Detektionssysteme abgedeckt
- Unzureichende **Nutzung** von Detektionssystemen
- Unzureichende **personelle Ressourcen**

### DER.1 Detektion von sicherheitsrelevanten Ereignissen – MUSS

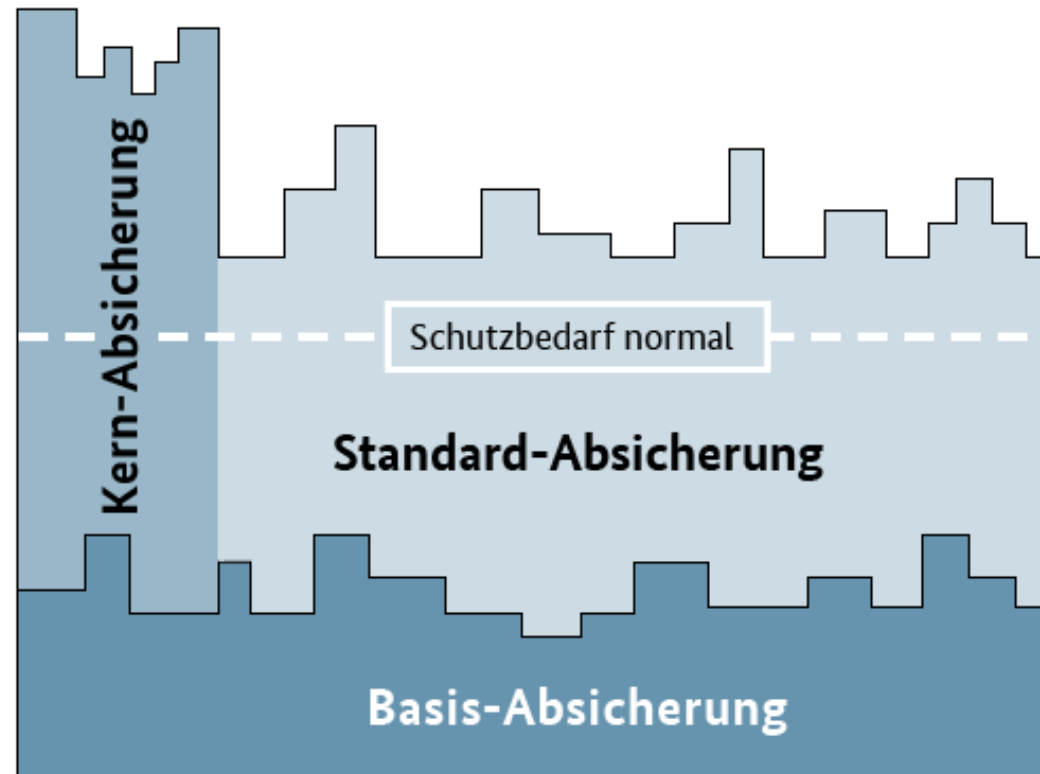
- Erstellung einer **Sicherheitsrichtlinie** für die Detektion von sicherheitsrelevanten Ereignissen
- Einhaltung **rechtlicher Bedingungen** bei der Auswertung von Protokollierungsdaten
- Festlegung von **Meldewegen** für sicherheitsrelevante Ereignisse
- **Sensibilisierung** der Mitarbeitenden
- Einsatz von mitgelieferten **Systemfunktionen** zur Detektion



**Voraussetzung:** OPS.1.5 Protokollierung, ORP.1 Organisation, OPS.1.1.4 Schutz vor Schadprogrammen,  
NET.3.2 Firewalls

## BSI Standards:

- BSI Standard 200-1: Managementsysteme für Informationssicherheit
- BSI Standard 200-2: IT-Grundschutz Methodik
- BSI Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz
- BSI Standard 200-4: Business Continuity Management  
(Notfallmanagement)



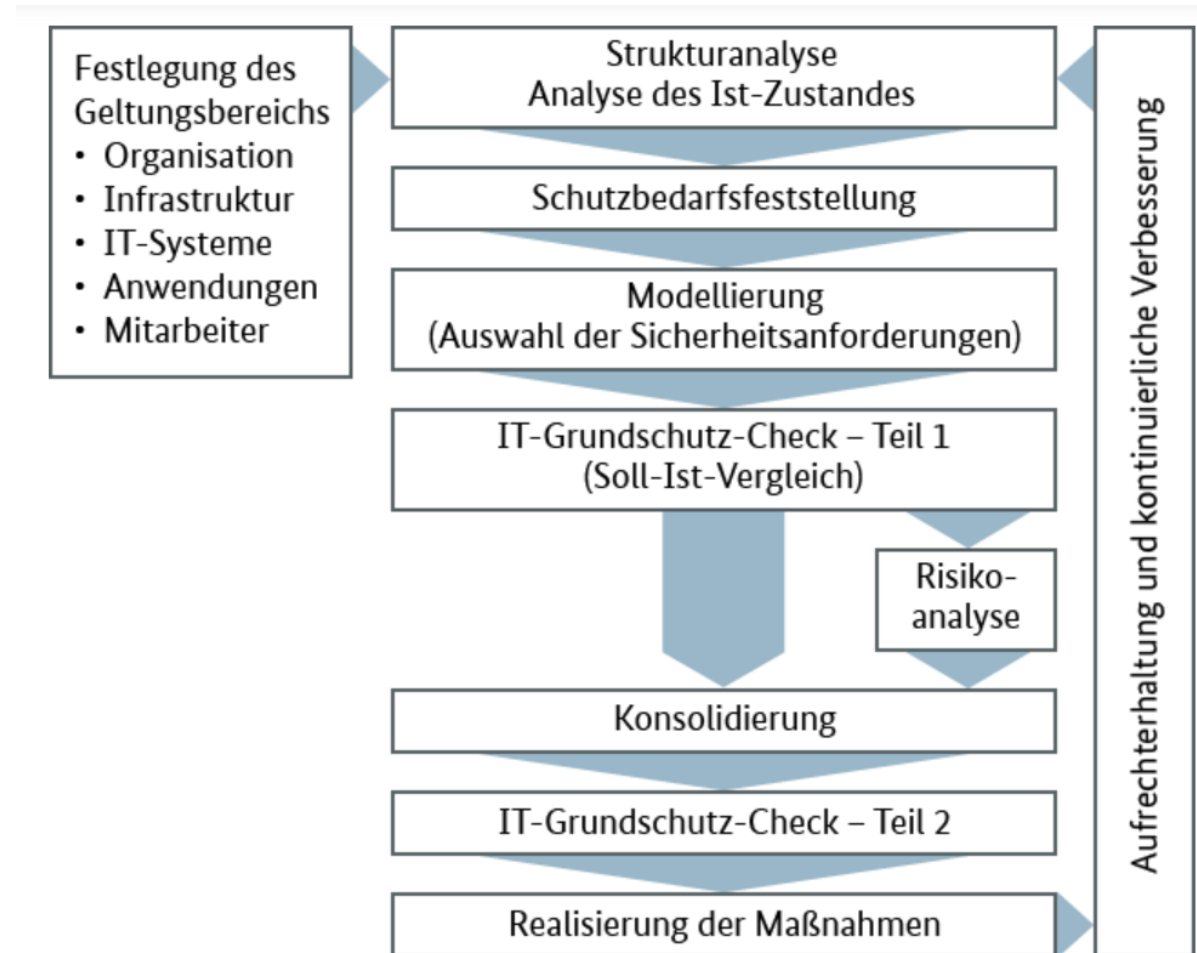


# Digitalverbund Bayern



HITS IS – Hochschulübergreifender IT-Service Informationssicherheit

## GRC – Governance, Risk, Compliance Tool



< Architektur

Assets ★

Work I

Exportieren

Importieren

Keine Tags ausgewählt

### Asset-Hierarchie

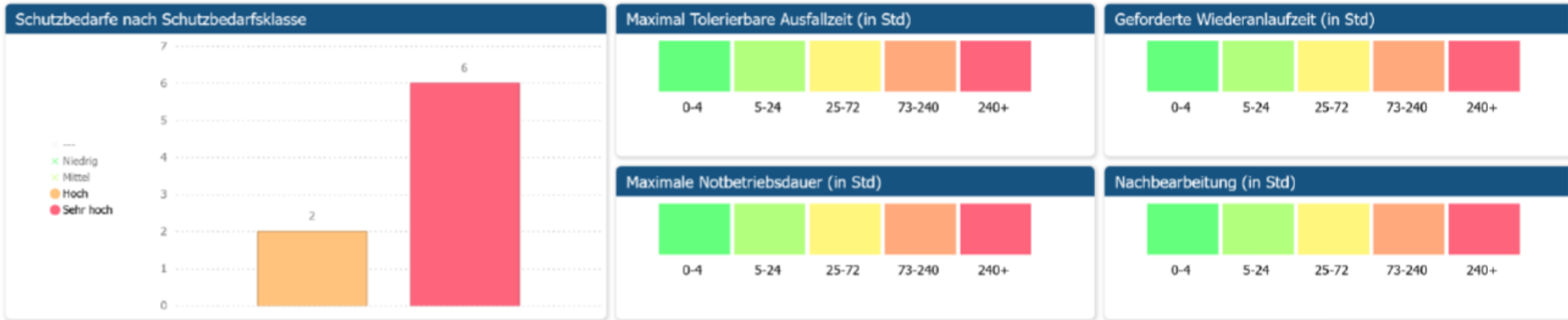
- ▼ DV - Bayern
  - ▶ 00 - Muster-Rahmenwerk
  - ▶ 00 - Musterhochschule
  - ▶ BSI - IT-Grundschutzprofil für Hochschulen
- ▼ FAU - Friedrich-Alexander-Universität Erlangen-Nürnberg
  - ▼ 01 - RRZE
    - HP - High Performance Computing
    - KS - Kommunikationssysteme
  - ▼ KU - Abteilung Kundenservice
    - ▶ KU01 - Dienst Clientbetreuung
      - W01 - Gruppe Windows Clients**
  - ▼ ZS - Zentrale Systeme
    - ▶ ZS01 - Dienst Server- und Systeminfrastruktur
      - ▶ ZS01\_1 - Backup & Archivierung
      - ▶ ZS01\_2 - Virtualisierung

### W01 - Gruppe Windows Clients

Details   Standardwerte (3)   Risiken   **Kontrollen**   Work Items (3)   Dokumentation (0)

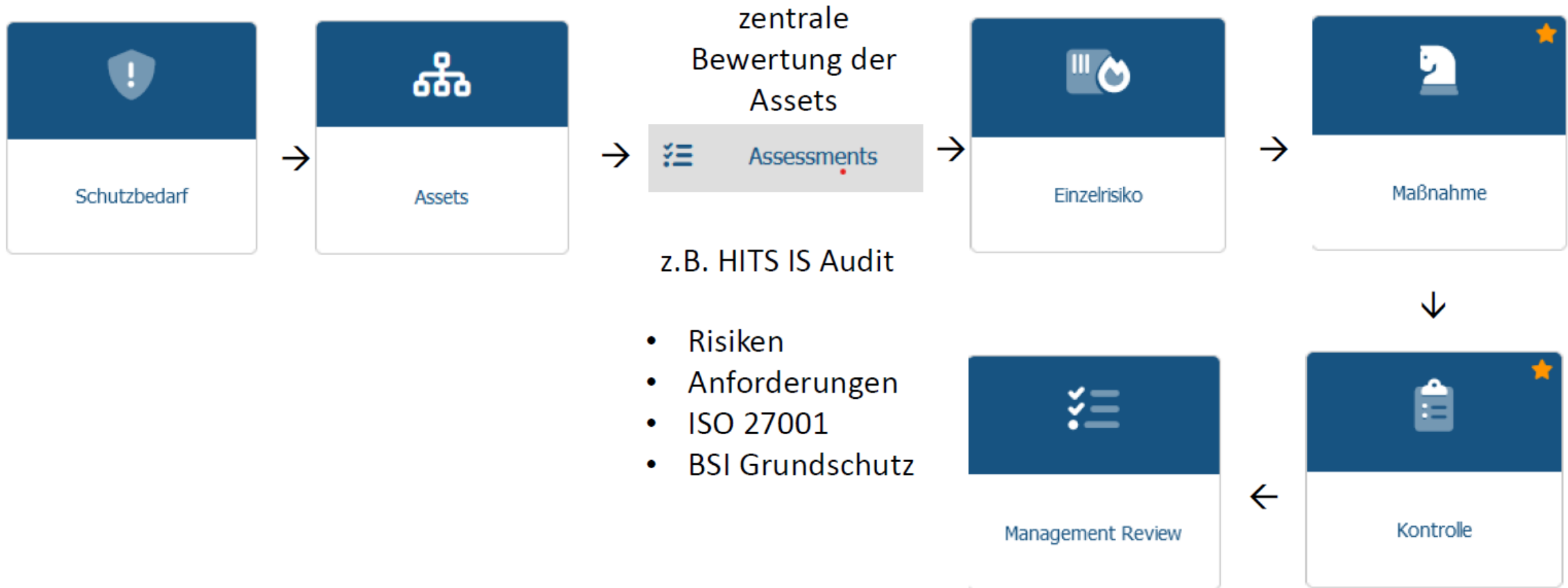
Nur ausgewählte anzeigen  

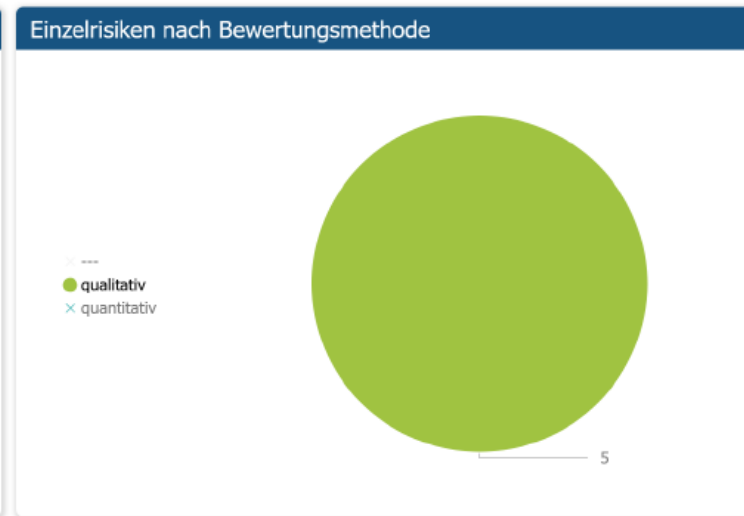
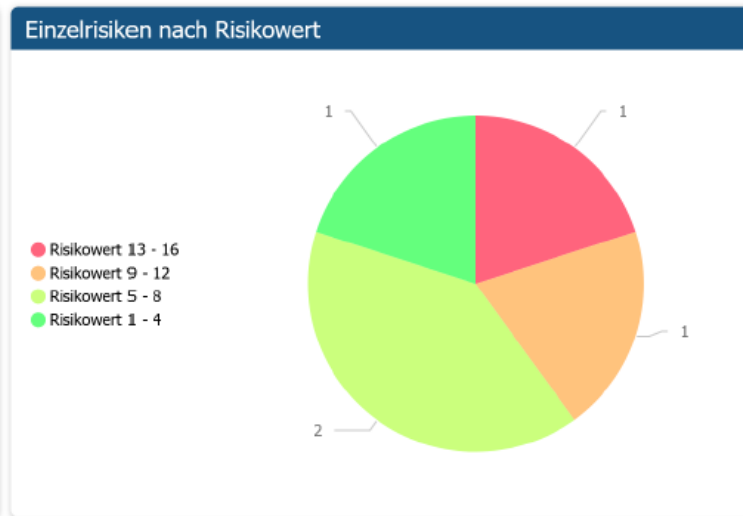
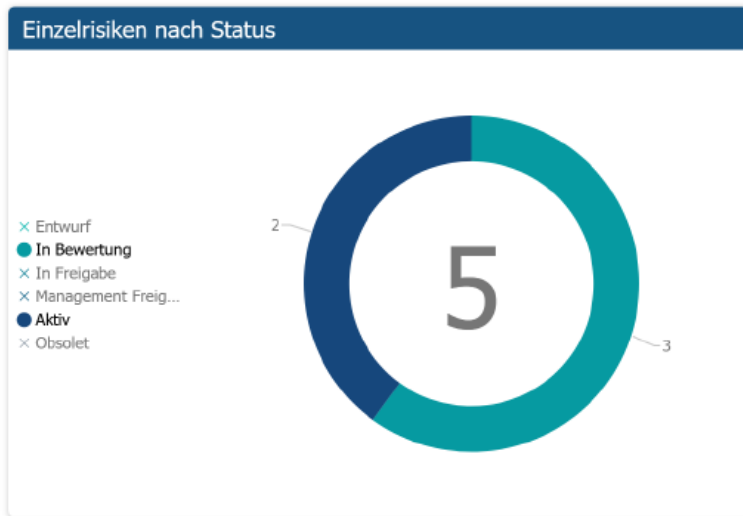
- ▼  BSI Anforderungen 2023
  - ▼  System-Bausteine
    - ▼  SYS IT-Systeme
      - ▼  SYS.2 Desktop-Systeme
        - ▼  SYS.2.2 Windows-Clients
          - ▼  SYS.2.2.3 Clients unter Windows
            - SYS.2.2.3.A5 Schutz vor Schadsoftware unter Windows (B)
            - SYS.2.2.3.A6 Integration von Online-Konten in das Betriebssystem (B) [Benutzende]
            - SYS.2.2.3.A9 Sichere zentrale Authentisierung in Windows-Netzen (S)
            - SYS.2.2.3.A12 Datei- und Freigabeberechtigungen unter Windows (S)
            - SYS.2.2.3.A15 Einsatz der Synchronisationsmechanismen unter Windows (S)
            - SYS.2.2.3.A16 Anbindung von Windows an den Microsoft-Store (S)
            - SYS.2.2.3.A17 Keine Speicherung von Daten zur automatischen Anmeldung (S)
            - SYS.2.2.3.A18 Einsatz der Windows-Remoteunterstützung (S)
            - SYS.2.2.3.A19 Sicherheit beim Fernzugriff über RDP (S) [Benutzende]
            - SYS.2.2.3.A20 Einsatz der Benutzerkontensteuerung UAC für privilegierte Konten (S)



Schutzbedarfe									
Element ID	Name	Primary Asset	Vertraulichkeit	Integrität	Verfügbarkeit	Verantwortlich	Status	letzte Änderu..	
PRQ0000003	Bewerbung und Zulassung	[BSI03/Z_Asset/Bewerbung und Zulassung]	●	●	●	Schneider Ute	● Aktiv	🗑	
PRQ0000009	Dienst Clientbetreuung	[KU01/Z_Asset/Dienst Clientbetreuung]	●	●	●	Test User	● Aktiv	🗑	
PRQ0000004	Immatrikulation und Studierendenmanagement	[BSI04/Z_Asset/Immatrikulation und Studieren...]	●	●	●	Schneider Ute	● Aktiv	🗑	
PRQ0000006	IT-Infrastruktur für Studierende	[BSI06/Z_Asset/IT-Infrastruktur für Studierende]	●	●	●	Schneider Ute	● Aktiv	🗑	
PRQ0000005	Prüfungen	[BSI05/Z_Asset/Prüfungen]	●	●	●	Schneider Ute	● Aktiv	🗑	
PRQ0000008	Service Server- und Systeminfrastruktur	[ZS01/Z_Asset/Dienst Server- und Systeminfras...]	●	●	●	Test User	● Aktiv	🗑	
PRQ0000001	Übergreifende Anwendungen (Basisdienste)	[BSI01/Z_Asset/Übergreifende Anwendungen (...]	●	●	●	Schneider Ute	● Aktiv	🗑	
PRQ0000002	Übergreifende Anwendungen (Clientdienste)	[BSI02/Z_Asset/Übergreifende Anwendungen (...]	●	●	●	Schneider Ute	● Aktiv	🗑	

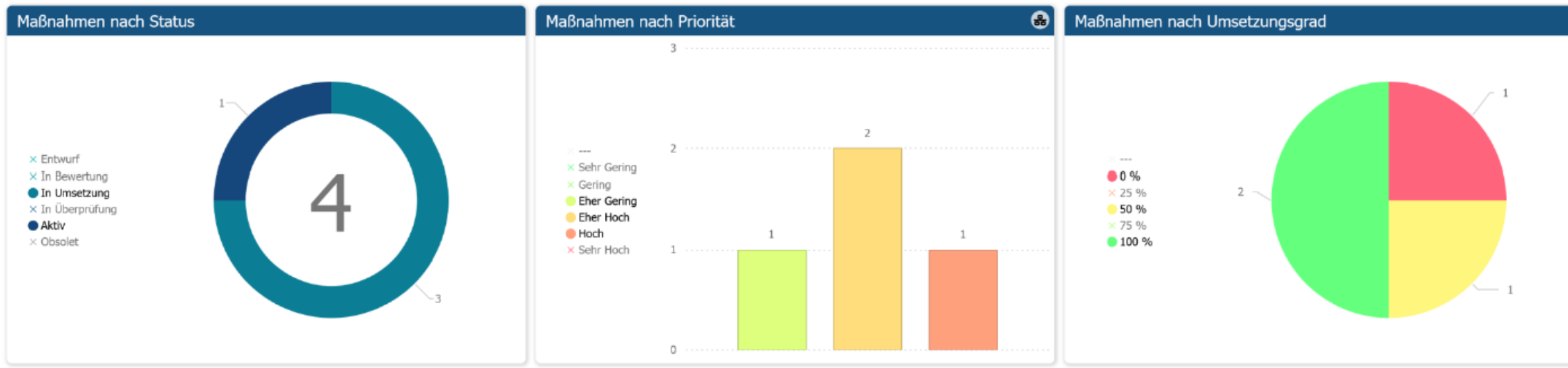
Geschäftsprozess	Beschreibung GP	Anwendungen (Plattform)	IT-Systeme	Räume
Immatrikulation und Studierendenmanagement	Immatrikulation bearbeiten	HISinOne STU ! (Alternativ: SAP SLcM Campusnet CampusOnline Primuss FactScience) APP. 3.1 APP. 3.2 APP. 4.2 APP. 4.3	Windows Server 2012 ! SYS. 1.1 SYS. 1.2.2	Allgemeines Gebäude INF.1
	Immatrikulation durchführen			
	Studierendendaten verwalten			
	Studierendenstatus verwalten			
	Studiengang- und Fachwechsel durchführen	Dakota (SMV) !	Linux Server ! SYS. 1.1 SYS. 1.3	Raum sowie Schrank für technische Infrastruktur ! INF.5
			Windows 10 Client ! (Plattform für Dakota) SYS. 2.1 SYS. 2.2.3	Verkabelung INF.12





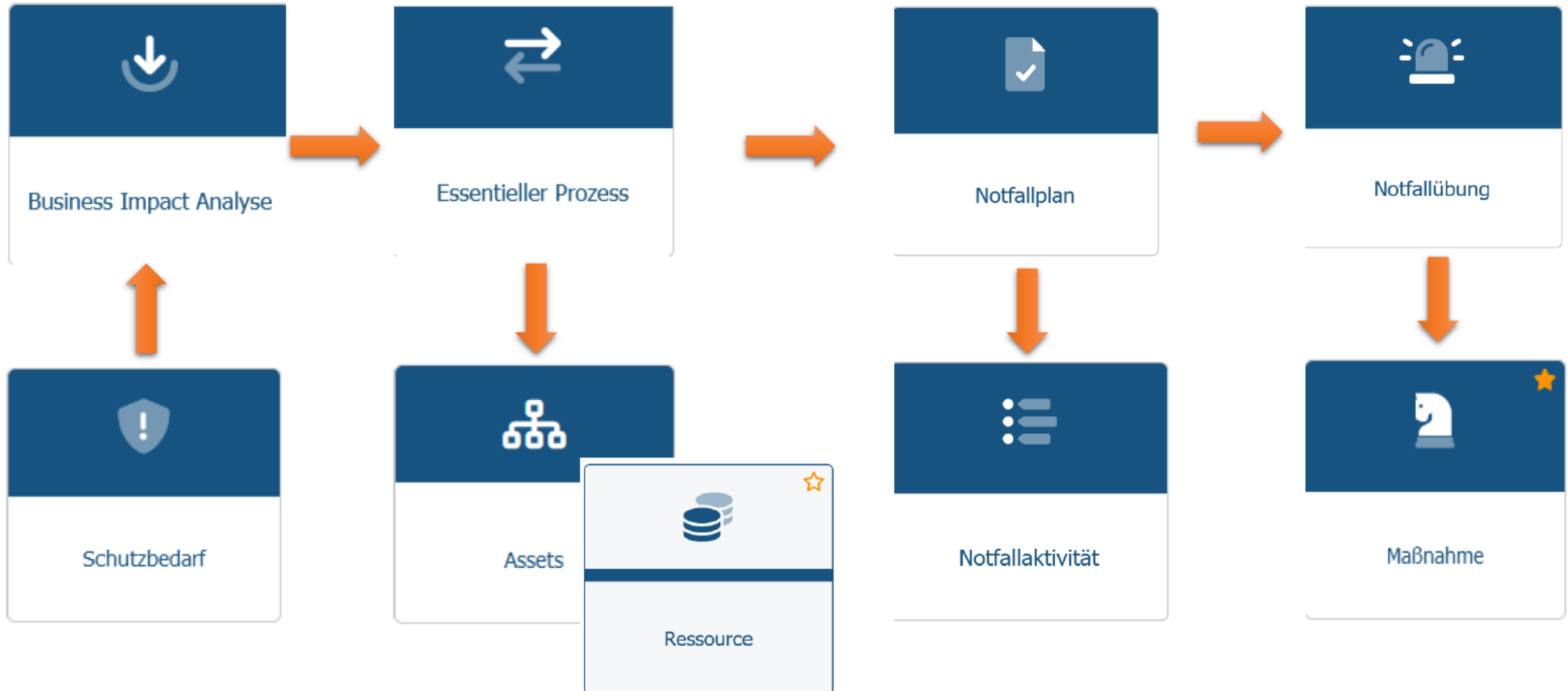
### Kontrollen & Maßnahmen nach Einzelrisiken

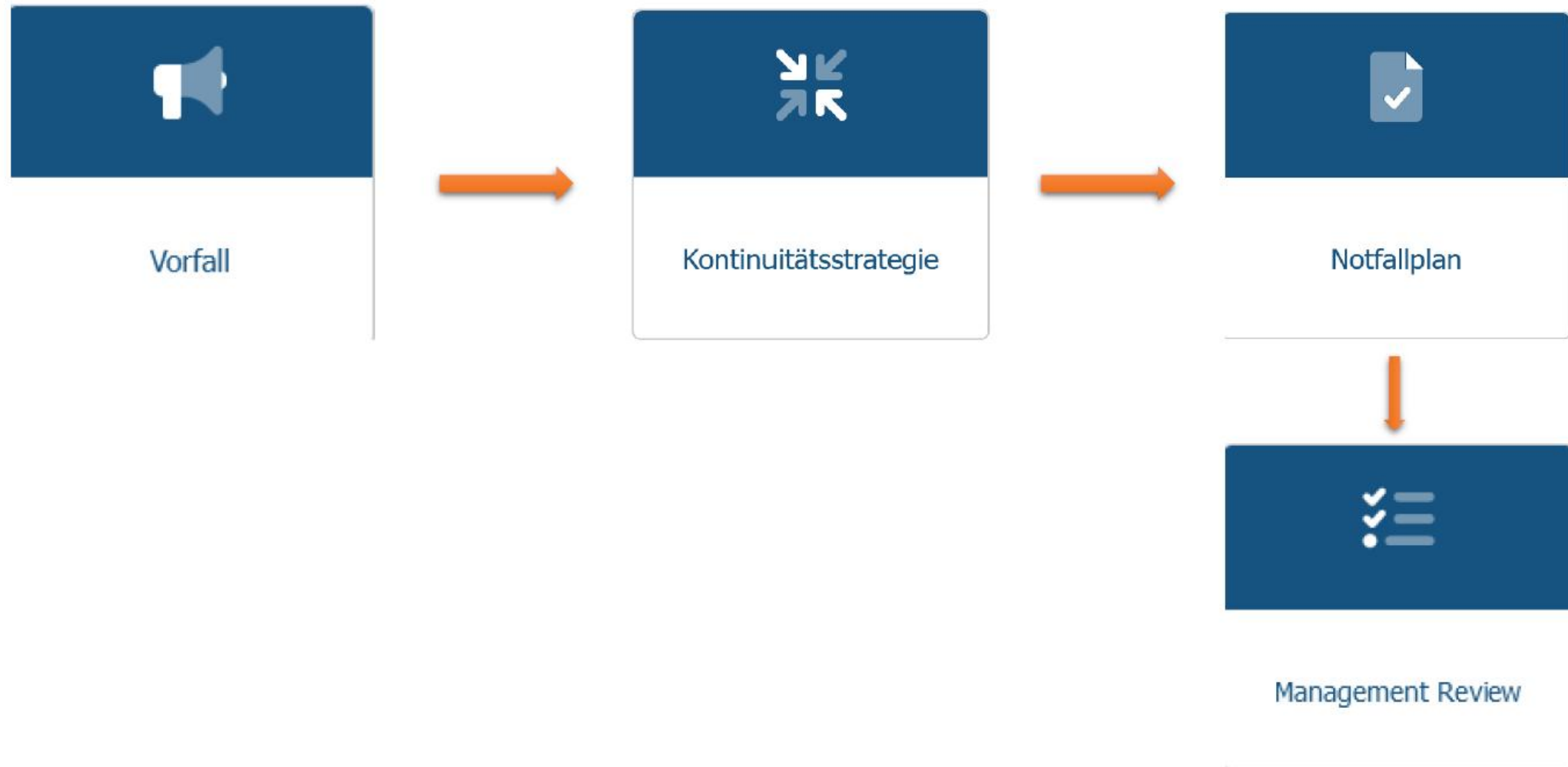
	Eleme...	Name	Bewertungsz...	Nächste B...		Eleme...	Name	Kontrolltyp	Kontrollst...		Eleme...	Name	Priorität der ...	Umsetzun...	let...
<input type="checkbox"/>	RSK00...	Fehlende Verfahren für d...	Jährlich	21.03.2025	<input type="checkbox"/>	CTR00...	Jährliche Überprüfung de...	Präventiv	Anwendbar	<input checked="" type="checkbox"/>	MEA0...	Erarbeitung eines Aware...	Hoch	0 %	<input type="checkbox"/>
<input type="checkbox"/>	RSK00...	Fehlende Verfahren zur R...	Jährlich	21.03.2025	<input type="checkbox"/>	CTR00...	Überprüfung der Klassifiz...	Präventiv	Anwendbar	<input checked="" type="checkbox"/>	MEA0...	Erstellen und Verabschie...	Eher Hoch	100 %	<input type="checkbox"/>
<input type="checkbox"/>	RSK00...	Ressourcenmangel IT-Sic...	Quartalsweise	21.06.2024											
<input type="checkbox"/>	RSK00...	Unzureichende Sicherheit...	Halbjährlich	22.09.2024											
<input type="checkbox"/>	RSK00...	Server(gruppe) Virtuelle ...	Quartalsweise	21.06.2024											

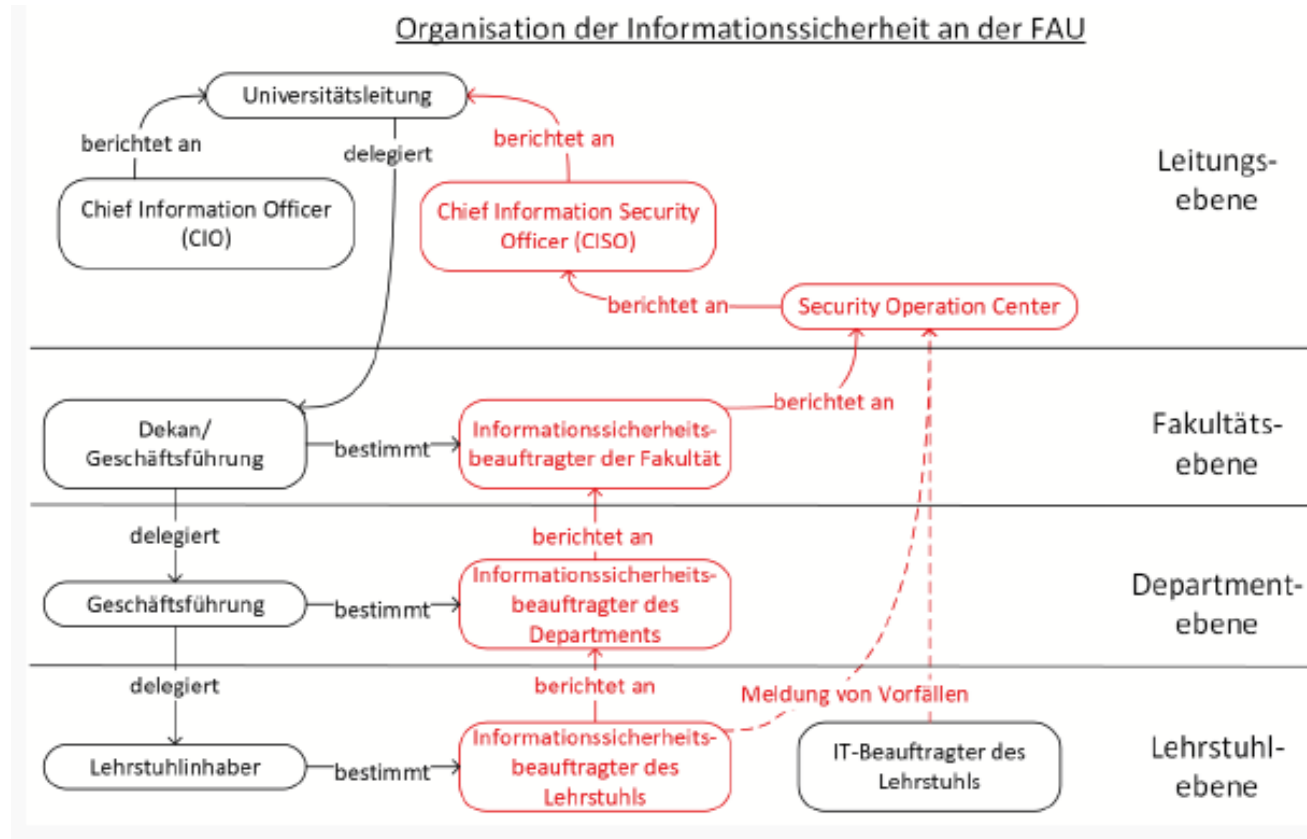


## Kontroll- & Maßnahmentestings nach Maßnahmen

	Element ID	Name	Priorität der Maßnahme	Umsetzungsgrad	letzte...
<input type="checkbox"/>	MEA00000...	Erarbeitung eines Awarenesskonzepts	Hoch	0 %	🕒
<input type="checkbox"/>	MEA00000...	Erstellen und Verabschieden einer akt...	Eher Hoch	100 %	🕒
<input type="checkbox"/>	MEA00000...	Überarbeiten der Organisationsrichtlinie	Eher Gering	50 %	🕒
<input type="checkbox"/>	MEA00000...	Überprüfung der Leitlinie auf Aktualität	Eher Hoch	100 %	🕒







---

**Vielen Dank für Ihre Aufmerksamkeit!**

**Fragen?**

**Freiwillige?**