Friedrich-Alexander-Universität
Technische Fakultät

FAU

# Informationssicherheit an der FAU nach BSI

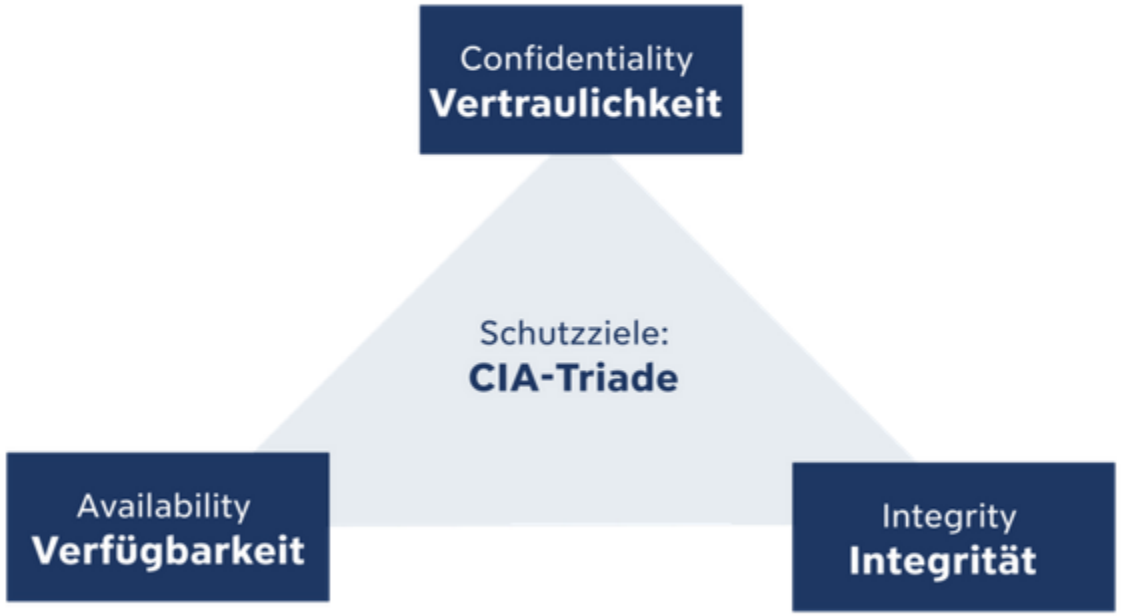
# Vorerst: neue Webseite

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.

# Standards und Normen

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

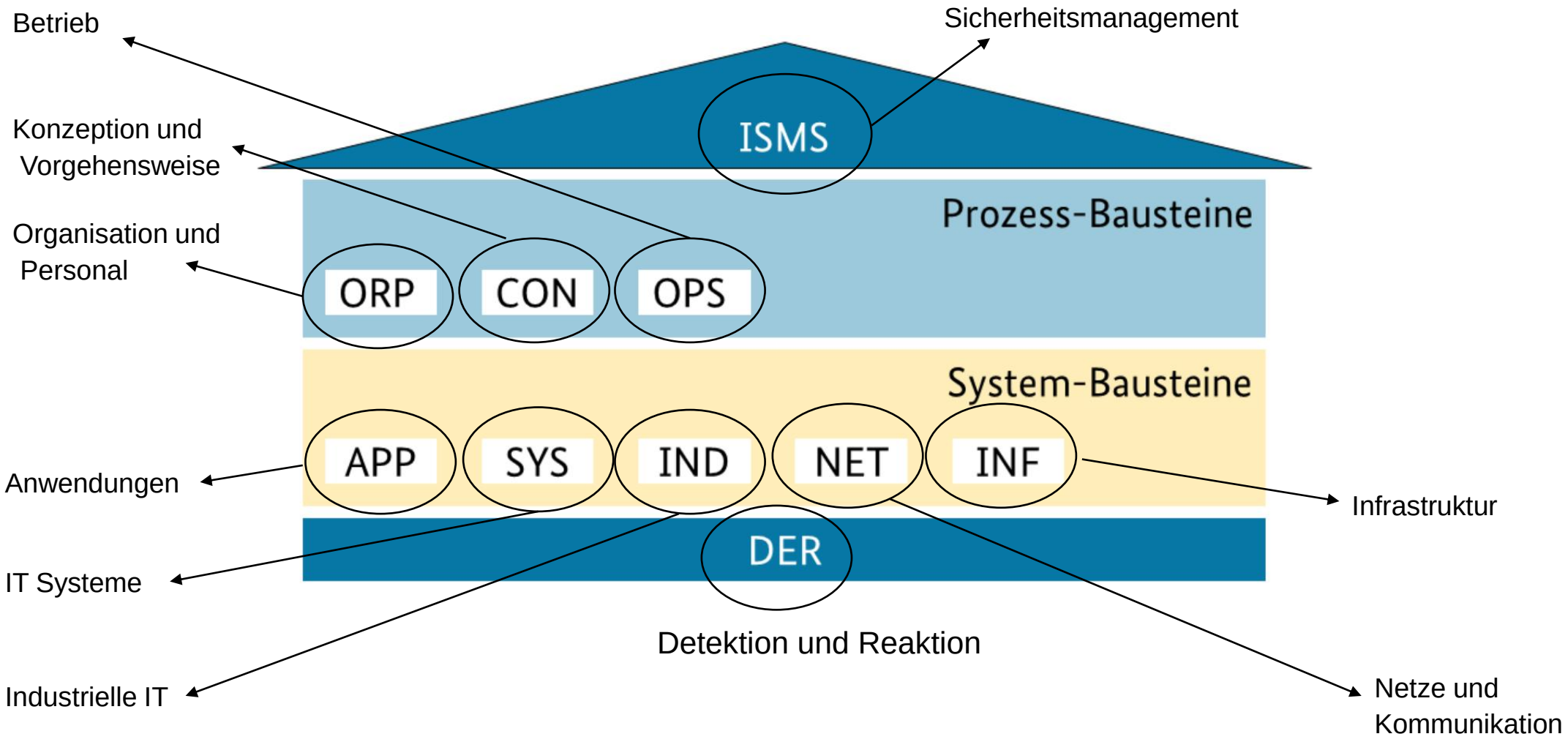
- Insbesondere: 27001, 27002, 27005

**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

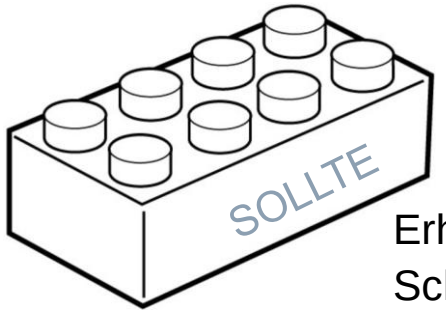
# BSI IT-Grundschutz Kompendium

## Bausteine

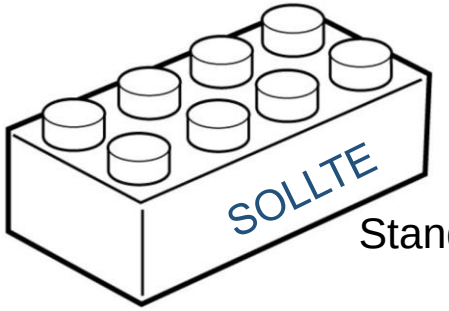


# BSI IT-Grundschutz

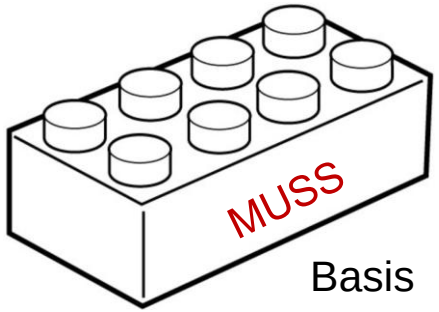
## Gefährdungen und Anforderungen




Erhöhter Schutzbedarf




Standard




Basis

Gefährdungslage

Ziel

## Priorität und Bearbeitungsreihenfolge

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

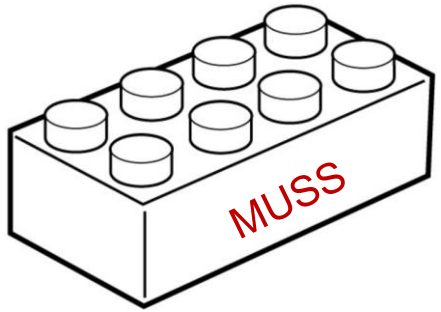
- Missachtung von gesetzlichen Vorschriften und betrieblichen Mitbestimmungsrechten
  - z.B. Sammlung und Auswertung von personenbezogener Informationen
- Unzureichende Qualifikation der Mitarbeitenden
  - z.B. nicht ausreichend geschult und sensibilisiert
- Fehlerhafte Administration der eingesetzten 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

# Incident Management nach BSI IT-Grundschutz

DER.1

## 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

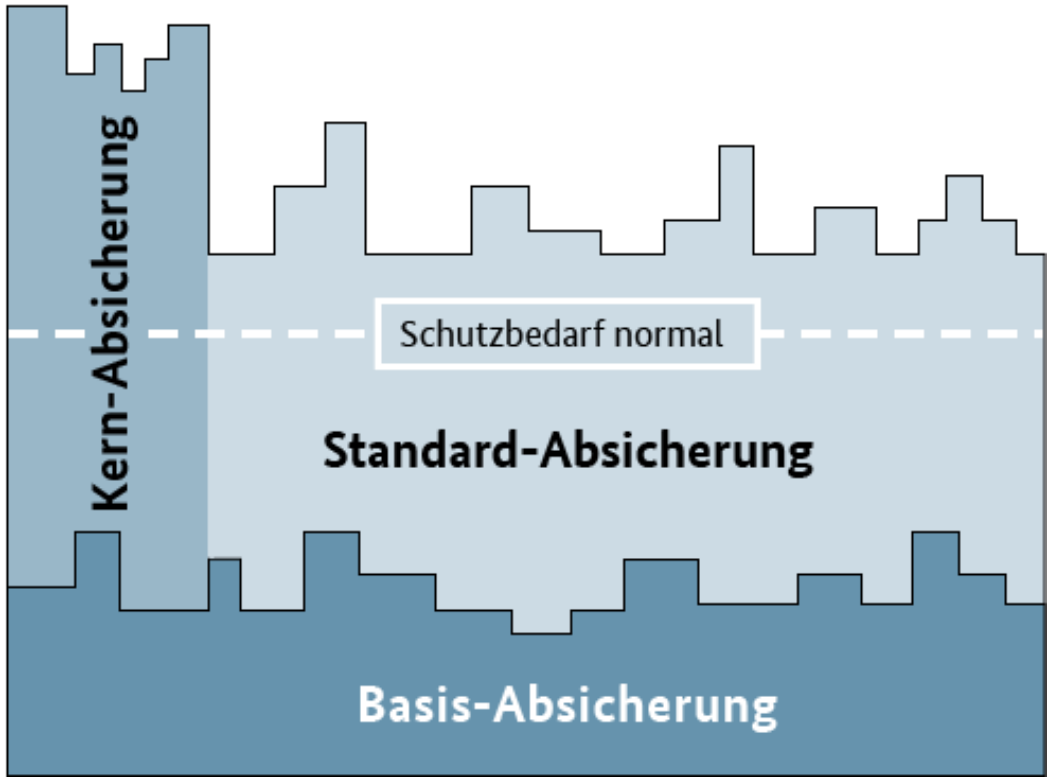
# BSI Standards

## BSI 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)

# BSI Standards

## BSI Standard 200-1: Managementsysteme für Informationssicherheit



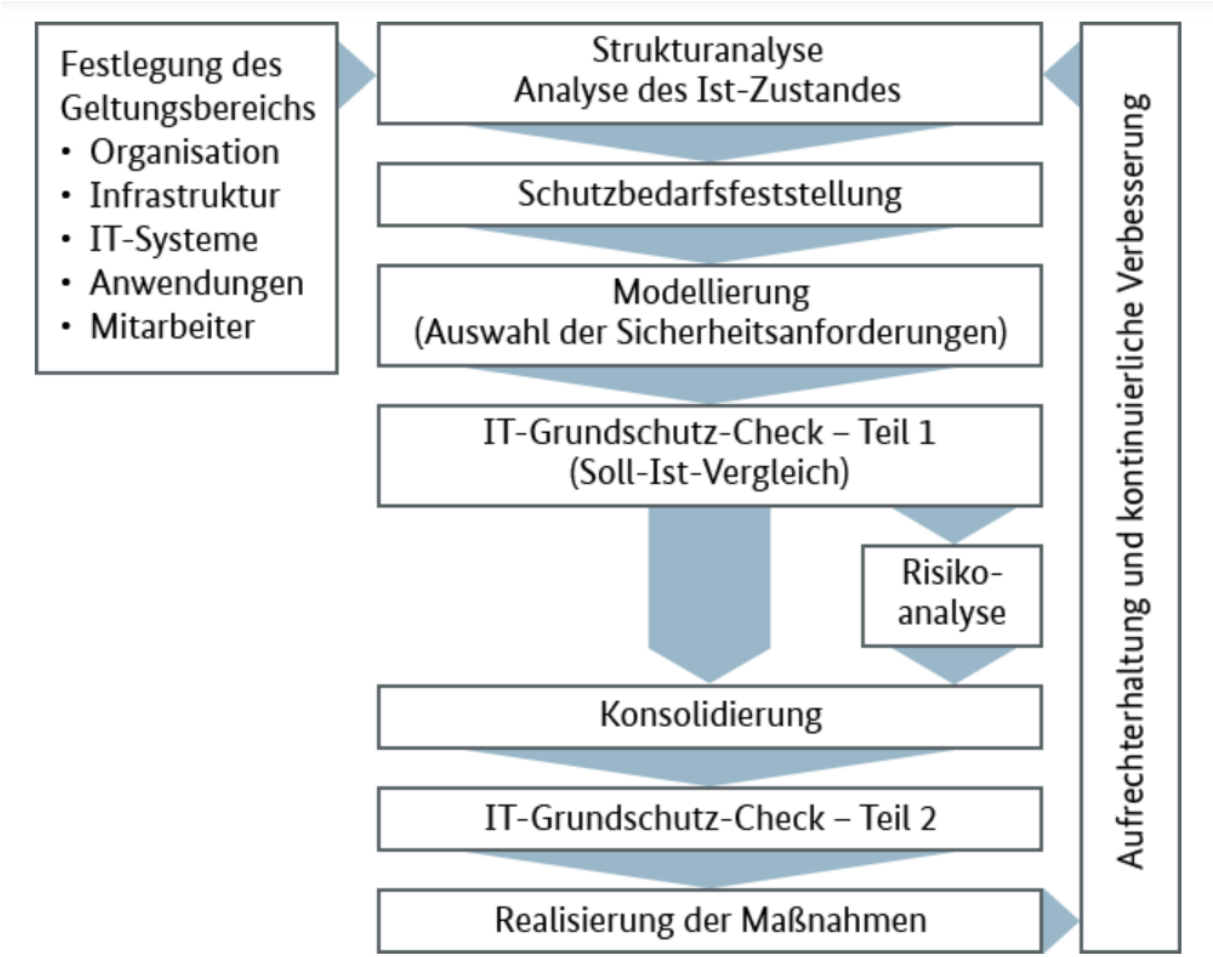
Digitalverbund Bayern

HITS IS – Hochschulübergreifender IT-Service Informationssicherheit

# GRC – Governance, Risk, Compliance Tool

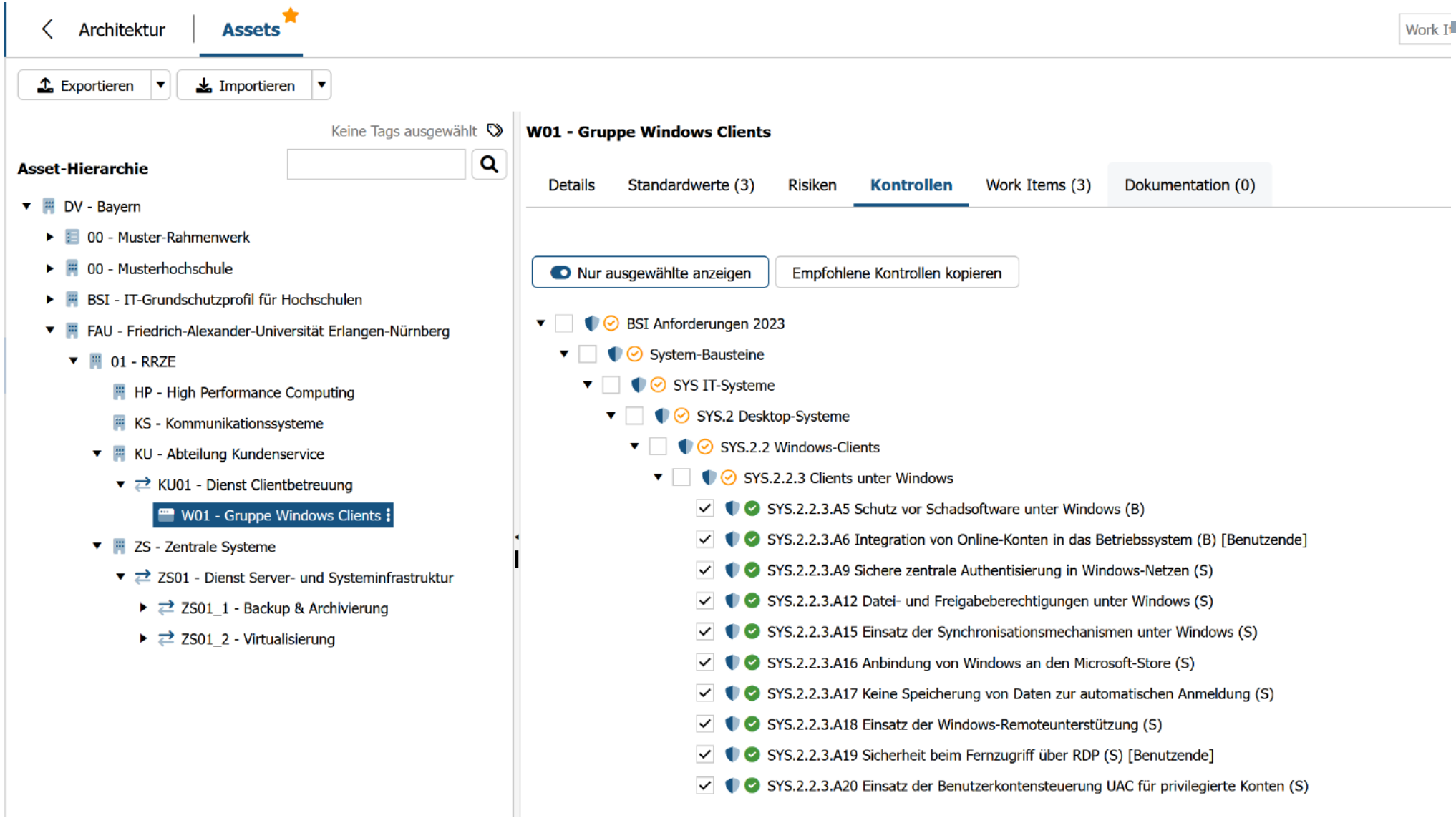
# IT-Grundschutz-Methodik

BSI-Standard 200-2



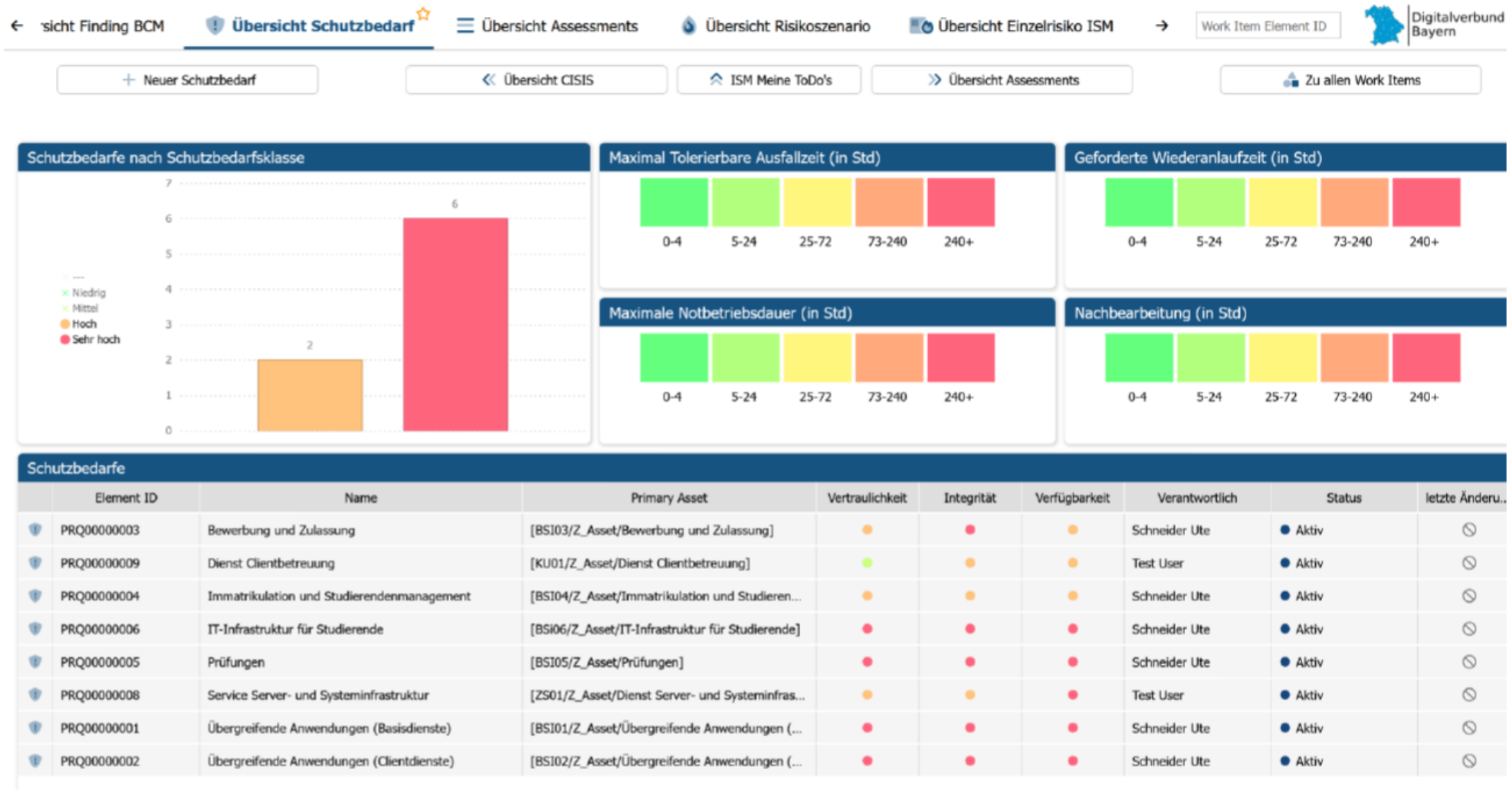
# ISMS

## Strukturanalyse & Modellierung



# ISMS

## Schutzbedarfsfeststellung



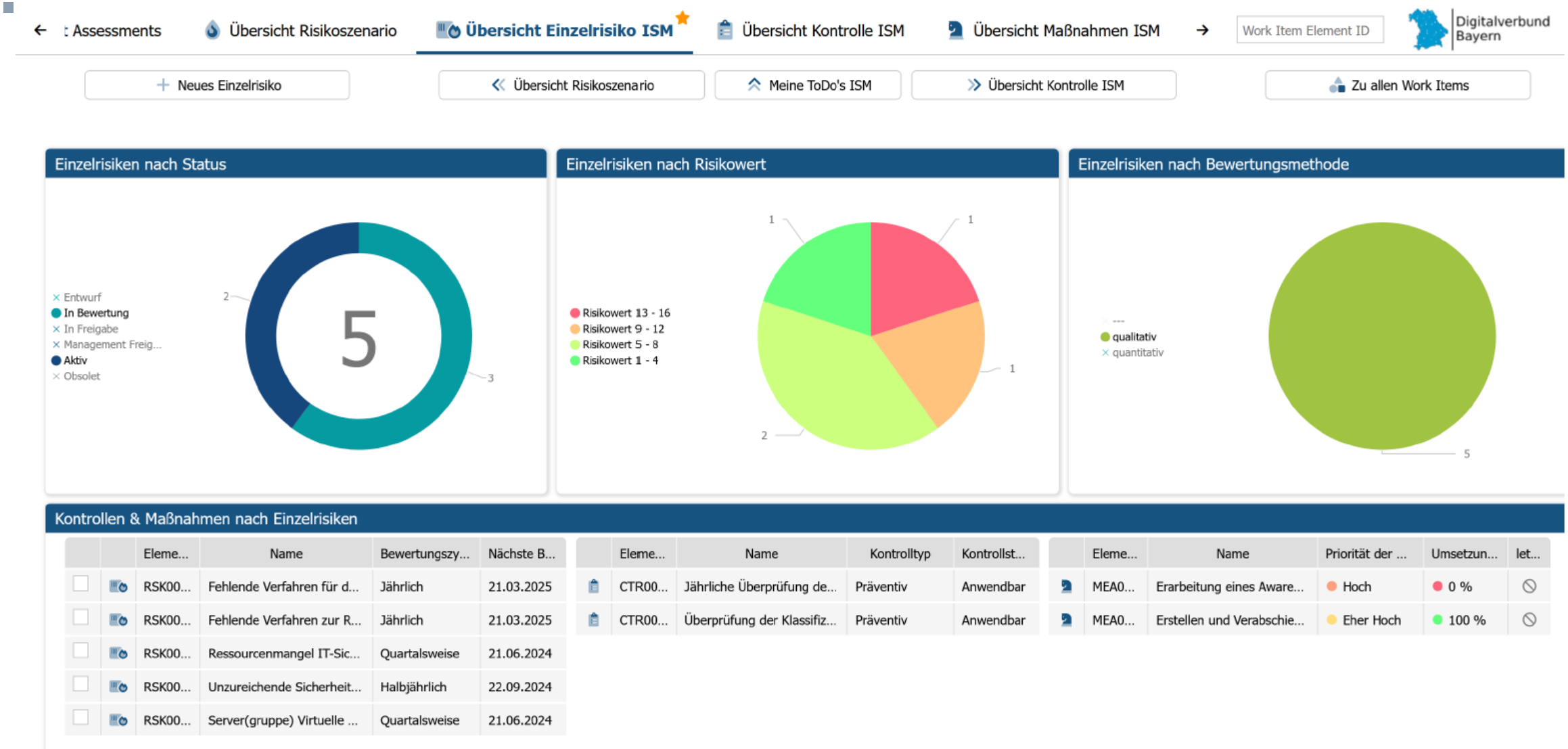
# Strukturanalyse

Hochschulprofil

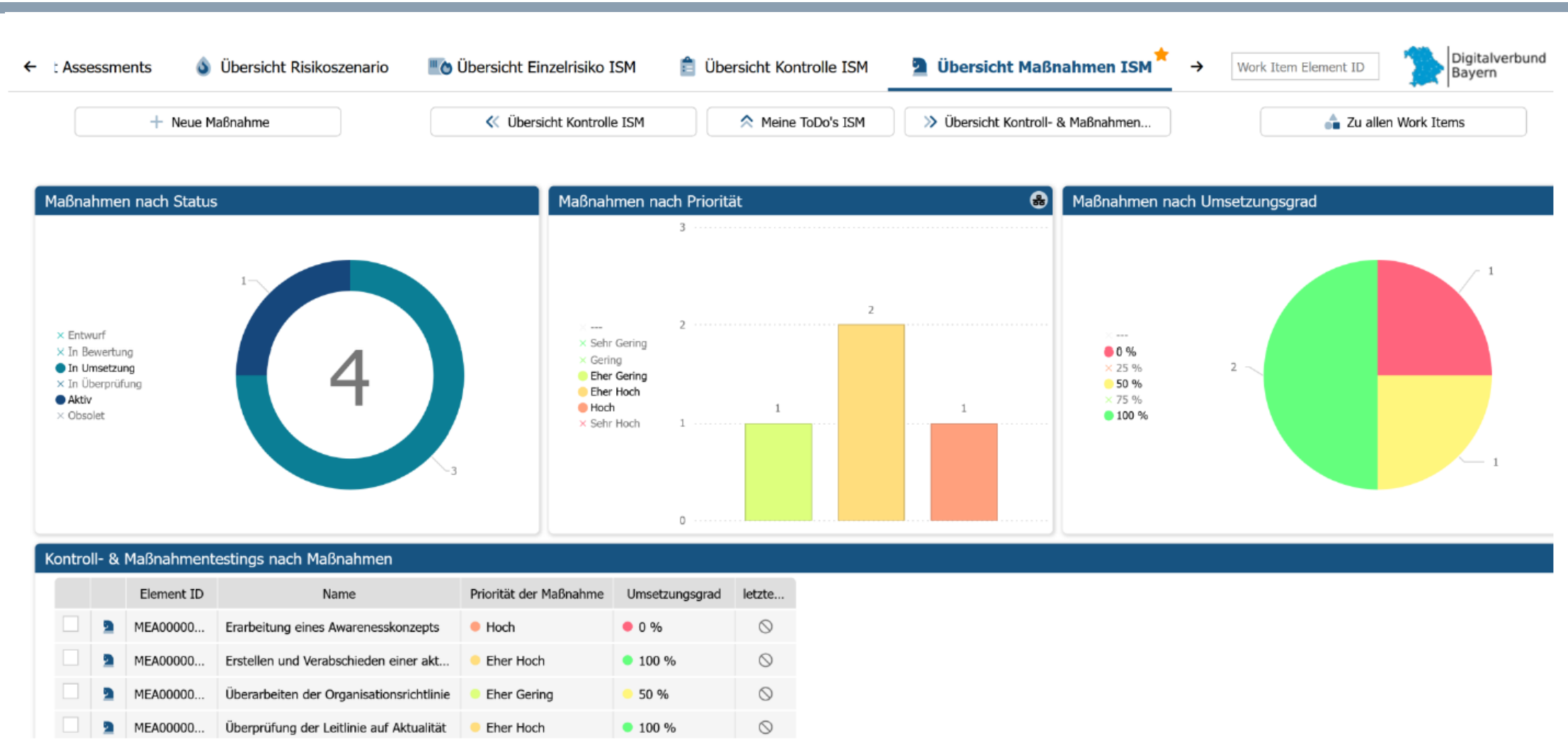
| Geschäftsprozess | Beschreibung GP | Anwendungen (Plattform) | IT-Systeme | Räume |
|---|---|---|---|---|
| Immatrikulation und Studierenden-management | Immatrikulation bearbeiten<br><br>Immatrikulation durchführen<br><br>Studierendendaten verwalten<br><br>Studierendenstatus verwalten<br><br>Studiengang-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

# Risikoanalyse

# Risikoanalyse



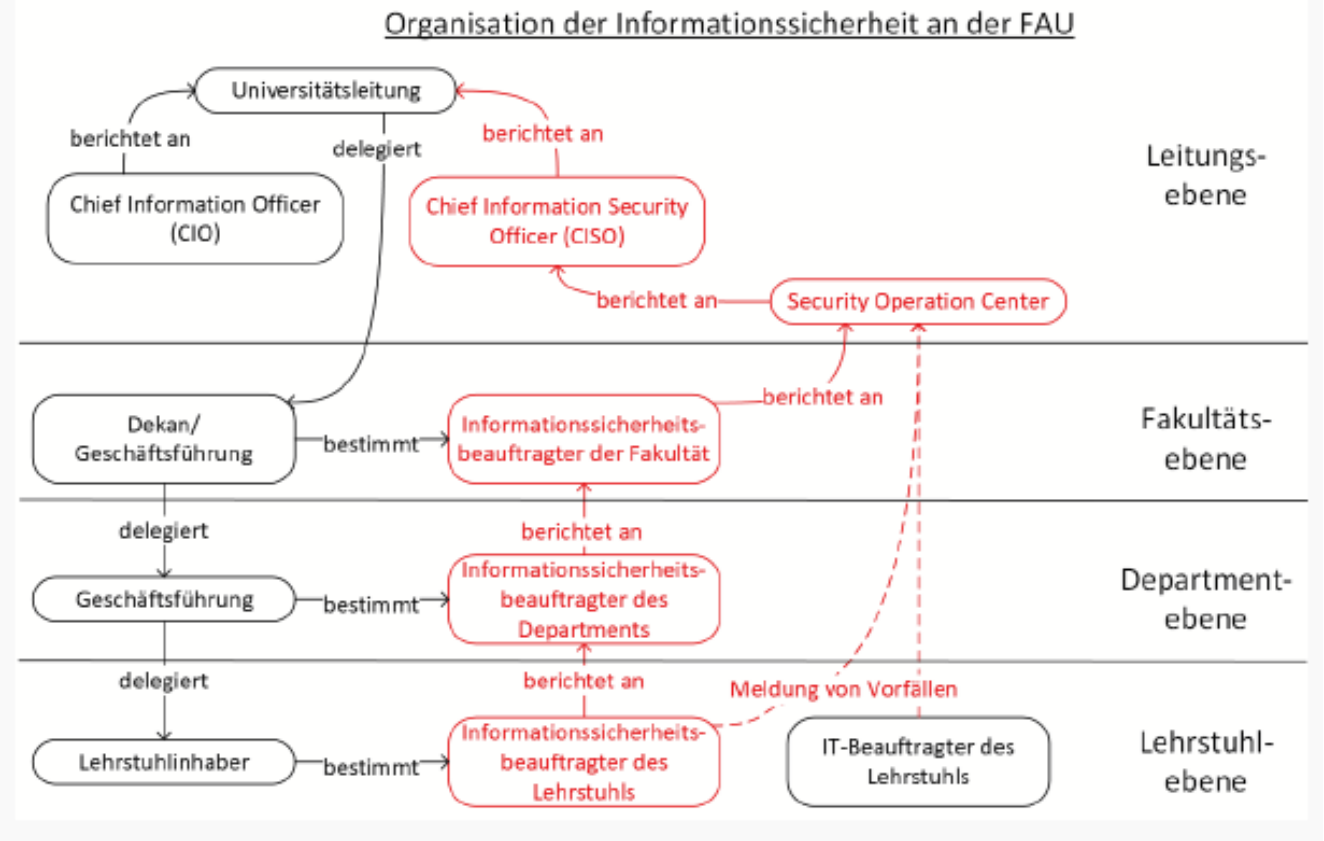
# Risikoanalyse: Maßnahmen



# Notfallmanagement: Notfallvorsorge

# Notfallmanagement: Notfallbewältigung

# Informationssicherheit an der FAU nach BSI



**Vielen Dank für Ihre Aufmerksamkeit!**

**Fragen?**

**Freiwillige?**