

# MIS - Medizinische Informationssysteme - 5BHBGM - SJ2021

[Startseite](#) / [Meine Kurse](#) / [HBGM](#) / [5BHBGM](#) / [MIS 5BHBGM 2021](#)

## [Ankündigungen](#)

[Microsoft Teams](#) Code: egjdixf

Login mittels Schul-Email & Passwort

## [Link zu Extamural \(PIR\)](#)

50% Abgaben, Wiederholungen, Mitarbeit während der Stunde, Präsentationen, Portfolioordner  
50% PLFs, Abgabegespräche

Wintersemester PLFs:

- \* 1. Termin: 21.10.2020 (Umsetzung von FHIR Ressource mit Model, Repository, Controller, Repository Test, Controller Tests, import.sql, Stoff laut Protokollen / Umsetzung der technischen Anforderung an die Organisation für die Abläufe eines Störungs- und Notfall-Prozess in einer Klinik, unter Berücksichtigung der DSGVO, des MPG und des NISG)
- \* 2. Termin: 23.12.2020 => gestrichen
- \* 3. PLF: 13.01.2021 ohne Lockdown, mit Lockdown auf 20.1.2021 verschoben.

---

### Sommersemester PLF:

17.3.2021 - 4h "Probematura" 7.-10.h (Stoffgebiet: FHIR Server, FHIR Client, Theoriefragen intramural, extramural Stoffgebiet entsprechend Mitschriften)

---

### Extra Unterricht

22.02.2021 - 11. und 12.h

---

## PLFs

 [PLF 1 1 DeviceRequest extramural Verspätete Abgaben werden ohne Ausnahme nicht bewertet](#)

 [Ergebnisse](#)

 [1. schriftliche Leistungsüberprüfung intramural](#)

Sehr geehrte Damen und Herren,

Sie bekommen 16 Fragen, die Sie in 20 beantworten müssen.

Sie können 100 Punkte erreichen

ACHTUNG:

15 Fragen haben 6 Punkte

1 Frage hat 10 Punkte

Die Leistungsüberprüfung wird automatisch nach 20 Minuten abgeschlossen.

Viel Glück!

Notenschlüssel:

1:100,0% - 87,6%

2:87,5% - 75,1%

3:75,0% - 62,6%

4:62,5% - 50,1%

5: 50,0% - 0%

 MÜ 1\_2 20.01.2021 (ohne node\_modules Ordner) Verspätete Abgaben werden ohne Ausnahme nicht bewertet

**Eingeschränkt** Nicht verfügbar, es sei denn: Sie sind in **Gruppe D**

 MÜ 1\_2 20.01.2021 (ohne node\_modules Ordner) Verspätete Abgaben werden ohne Ausnahme nicht bewertet

**Eingeschränkt** Nicht verfügbar, es sei denn: Sie sind in **Gruppe C**

 [MÜ 1\\_2 20.01.2021 \(ohne node\\_modules Ordner\) Verspätete Abgaben werden ohne Ausnahme nicht bewertet](#)

 MÜ 1\_2 20.01.2021 (ohne node\_modules Ordner) Verspätete Abgaben werden ohne Ausnahme nicht bewertet

**Eingeschränkt** Nicht verfügbar, es sei denn: Sie sind in **Gruppe A**

---

## MIS Intramural / DL-Selbstüberprüfung

Sehr geehrte Schülerinnen und Schüler,

anbei finden Sie 3 Fragen, die Sie in 8 Minuten (pro Frage) als Wissensüberprüfung beantworten sollen.

Bitte, versuchen Sie die Fragen "ohne Hilfsmitteln" eigenständig zu beantworten.

Jede Frage hat 100 Punkte, die auf die richtigen Antworten aufgeteilt sind.

Mit freundlichen Grüßen

F. Hoheiser-Pförtner

 [DL-Selbstüberprüfung 1. Teil](#)

 [DL-Selbstüberprüfung 2. Teil](#)

 [DL-Selbstüberprüfung 3. Teil](#)

---

## MIS Intramural / Mitschriften (Hoheiser-Pförtner)

 [Mitschriften 1. + 2. Semester im Schuljahr 2020/2021 - Intramural](#)

**Die MITSCHRIFTEN werden zur Mitarbeitsnote gezählt!**

Bitte legen Sie die Mitschriften nach folgender Regel ab:

<JJJJMMTT>\_<#>\_MIS\_4AHBGM\_<FAMILIENNAME1>\_<FAMILIENNAME2>.DOC

JJJJ = z.B.: 2019, MM = z.B.: 09, TT = z.B.: 18

# = 1, 2, 3, ... Datei am Tag - wird nach der Reihenfolge der Erzeugung nummeriert.

Achtung: Dieser Dateiname steht auch in der Zeile der MITSCHRIFTEN\_LISTE.

Sie erstellen eine Liste mit EXCL mit der Bezeichnung MITSCHRIFTEN\_LISTE\_SJ1920.XLS mit folgenden Spalten bzw. Spaltenüberschriften

1. Spalte: **Tag der Mitschrift** in Form JJJJMMTT

2. Spalte: **fortlaufende Nummer am Tag**

3. Spalte: **Familiennamen 1. Autorin / Autor** (Familiennamen muss eindeutig sein)

4. Spalte: **Familienname 2. Autorin / Autor** (Familienname muss eindeutig sein)

5. Spalte: **Dateiname der Mitschrift**

6. Spalte: **Anmerkungen**

Vorgangsweise für die Mitschrift:

Jede Unterrichtseinheit (= 1 Doppelstunde) wird von 2 Personen eine Mitschrift erzeugt.

Jede Unterrichtseinheit sind 2 andere Person für die Mitschrift verantwortlich.

Es gibt ein Liste welche Personen in welcher Unterrichtseinheit für die Mitschrift verantwortlich sind bzw. waren und welche Mitschrift von diesen erzeugt wurde. Diese Personen sind auch für die Wartung der Mitschriften-Liste verantwortlich.

Sie achten auf eine gleichmäßige Verteilung der Personen, die die Mitschriften erzeugen.

Fällt die Mitschrift in eine Unterrichtseinheit aus, dann werden die Personen auf die nächste Einheit verschoben.

**Die MITSCHRIFT ist Einheitlich mit Kopf- und Fußzeile (KW, Autorinnen/Autoren, Datum, Nummer, Kurzzusammenfassung, Inhalt, ergänzende Informationen).**

Wenn Sie in ihren Mitschriften eine andere Quelle verwenden, dann muss diese mit einer Quellenangabe

"<https://de.wikipedia.org/wiki/Quellenangabe>, Stand: 06.09.2019" angeführt werden.

Danke Hoheiser-Pförtner

 Falsche Maßnahmen oder Fehler der Personen

SEIT DER USB-ATTACKE NEHMEN WIR  
DIE ABSICHERUNG DES SERVERRAUMS SEHR ERNST.





Quelle: IT-Sicherheit und Datenschutz im Gesundheitswesen (ISBN 978-3-658-21589-7)

Sie müssen immer damit rechnen, dass Ihre Maßnahmen nicht greifen oder die Personen, die die IKT nutzen, einen Fehler machen.

## Beurteilung von Richtlinien: RICHTIG oder FALSCH?

Die Beispiele sollen Ihnen verschiedene Möglichkeiten aufzeigen, wie eine Richtlinie aufgebaut und die Überlegungen bei der Beurteilung sein kann.

### Richtlinie für KRITIKALITÄTSANALYSE:

*Bei der Kritikalitätsanalyse werden aus der Prozessübersicht des SPITALS diejenigen Prozesse ausgewählt, deren Ausfall oder Störung zu schwerwiegenden Verletzungen der Schutzziele der Gesundheitseinrichtung führen würden.*

**Diese Prozesse werden als kritische Prozesse bezeichnet.**

*Zur Auswahl der kritischen Prozesse sind folgende Kriterien entscheidend:*

1. die Auswirkungen eines Prozessausfalls auf Leben und Gesundheit,
2. der Umfang eines Prozessausfalls,
3. die gesetzliche, vertragliche oder gesellschaftspolitische Relevanz der Ausfallsfolgen und dabei
  - 3a. die potenziellen Auswirkungen der Verletzung der Vertraulichkeit von personenbezogenen Daten für die betroffene Person,
  - 3b. die Ausfallszeit (Minuten, Stunden, Tage), an dem die Auswirkungen eines Ausfalls als kritisch anzusehen ist,
4. die mit einem Ausfall verbundenen wirtschaftlichen Schäden.

*Bei der Kritikalitätsanalyse werden Bedrohungen ermittelt, die die Prozesse nach den oben angeführten Kriterien beeinflussen.*

1. Warum ist diese Richtlinie **RICHTIG** ist oder **FALSCH**.
2. Warum ist z.B. die Bedrohung "RANSOMWARE" als kritisch, für einen Prozesse in der Gesundheitsversorgung im Spital zu bewerten.

### Dokumentenlenkung-Beschreibung

Dieses Dokument ist ein Muster. Die Inhalte sind als Gedankenstütze für die Leserin oder den Leser gedacht. Nicht alle Punkte müssen in Ihren Ausarbeitungen vorkommen. Die Kopf-/Fußzeile muss von Ihnen angepasst werden. Sie können noch ein Deckblatt einfügen. Der Inhalt ist nicht vollständig und einige Punkte können in der Realität abweichen

Die **High Level Structure** hat eine starke Fokussierung auf Management-Systeme:

Die Struktur (**PLAN DO CHECK ACT**) besteht immer aus zehn Kapiteln:

1. Anwendungsbereich
2. Normative Verweisungen
3. Begriffe
4. **Kontext der Organisation**
5. **Führung**
6. **Planung (für das Managementsystem)**
7. **Unterstützung**
8. **Betrieb**
9. **Bewertung der Leistung**
10. **Verbesserung**

Diese Struktur soll Ihnen helfen, den Aufbau Ihrer Dokumente entsprechend zu gestalten.

Sie sollten dabei folgende Überlegungen beachten:

Beschreiben Sie in Ihren Ausführungen immer den Ablauf **PLAN DO CHECK ACT**.

**PLAN:**

Welches Gremium (Geschäftsleitung, verantwortliche Person für Informationssicherheit, Datenschutz, Medizintechnik, ...) entscheidet über den Inhalt der Dokumente.

**DO:**

Welche Maßnahmen sollen im Betrieb umgesetzt werden.

**CHECK:**

Wie erfolgt die Überprüfung dieser Maßnahmen.

**ACT:**

Welche Verbesserungen sind notwendig.

---

## Netz- und Informationssystemsicherheitsgesetz – Risiko im Gesundheitswesen

Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)

Die wichtigste Maßnahme der Europäischen Cybersicherheitsstrategie der EU ist die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union ("NIS-Richtlinie"). Sie zielt darauf ab, ein höheres Sicherheitsniveau von Netz- und Informationssystemen in der ganzen EU zu erreichen.

Österreich setzt die europäische NIS-Richtlinie mit dem Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG) um. Dabei werden Aufgaben, die sich aus der NIS-Richtlinie ergeben, bereits bestehenden Strukturen übertragen.

Die vorliegende Seite stellt allgemeine Informationen über das NISG bereit und soll wichtige Fragen beantworten. Darüberhinausgehende Informationen können unter den jeweiligen Webseiten des Bundeskanzleramts und des Bundesministers für Inneres abgerufen werden.

Quelle: <https://www.nis.gv.at/...>

## Verfügbarkeit eines Rechenzentrums

Bei der Erstellung und Erweiterung oder auch Überprüfung eines IKT-Konzeptes ist heute von entscheidender Bedeutung, wie **die Verfügbarkeit der IKT-Infrastruktur** des Unternehmens, der Organisation, des Krankenhauses usw. eingeschätzt wird. Die sich daraus ergebende Grundsatzfrage lautet:

**"Wie hoch ist die maximale tolerierbare Ausfallzeit der IKT-Infrastruktur des Unternehmens, der Organisation, des Krankenhauses usw. ?"**

Eine Forderung nach hoher Verfügbarkeit beinhaltet jedoch nicht nur die Auseinandersetzung mit technischen Lösungsmöglichkeiten, sondern verlangt vom Betreiber bzw. der Betreiberin auch Ansätze und Ausführungen für eine umfassende organisatorische Struktur.

Verfügbarkeitsklasse	Verfügbarkeit	Kumulierte, wahrscheinliche Ausfallzeit pro Jahr	Auswirkung
VK 0 ca. 95%	keine Anforderungen	ca. 2-3 Wochen	Hinsichtlich der Verfügbarkeit sind keine Maßnahmen zu treffen. Die Realisierung des IT-Grundschatzes für die anderen Grundwerte wirkt sich förderlich auf die Verfügbarkeit aus.
VK 1 99,0%	NORMALE	weniger als 90 Std.	Hinsichtlich der Verfügbarkeit erfüllt die einfache Anwendung des IT-Grundschatzes (BSI 200-1 und BSI 200-2) die Anforderungen
VK 2 99,9%	HOHE	weniger als 9 Std.	Die einfache Anwendung des IT-Grundschatzes ist zu ergänzen durch die Realisierung der für hohen Verfügbarkeitsbedarf empfohlenen Bausteine, z. B. die Bausteine B 1.3 Notfallvorsorge, B 1.8 Behandlung von Sicherheitsvorfällen und die Anwendung der Risikoanalyse auf der Basis von IT-Grundschatz (BSI 200-3).
VK 3 99,99%	SEHR HOHE	unter 1 Std.	Realisierung der nach IT-Grundschatz für ausgewählte Objekte empfohlenen Maßnahmen mit besonderem Einfluss auf den Grundwert Verfügbarkeit, z. B. die Maßnahme M 1.28 USV im Serverraum oder M 1.56 Sekundär-Energieversorgung im Rechenzentrum, ergänzt durch HV-Maßnahmen aus dem HV-Kompendium
VK 4 99,999%	HÖSTE	ca. 5 Min.	IT-Grundschatz ergänzt durch Modellierung nach dem HV-Kompendium. IT-Grundschatz als Basis wird zunehmend durch HV-Maßnahmen ersetzt und ergänzt.
VK 5 100%	DISASTER TOLERANTE	keine	Modellierung nach dem HV-Kompendium. IT-Grundschatz dient weiterhin als Basis für die vorstehenden Bereiche sowie die anderen Schutzwerte Integrität und Vertraulichkeit.

Quelle: Leitfaden Betriebssicheres rechenzentrum (Version 3) Autor: BITKOM

## Prozesse für (IT-)Störfallbehandlungen werden immer WICHTIGER!

Der Gesetzgeber hat seit vielen Jahren Safety und Security im Gesundheitssektor in verschiedenen Gesetzen verankert, wie z. B. dem Gesundheitstelematikgesetz 2012 (GTeIG 2012), dem Medizinproduktegesetz (MPG) sowie seit 2018 in der Datenschutzgrundverordnung (DSGVO) und im Netz- und Informationssystemsicherheitsgesetz (NISG). Besonders „Security & Privacy by Design & Default“ sind, neben den Abstimmungen der involvierten Personen (z. B. anhand der ISO/IEC 27000-Serie und/oder der ISO/IEC 80001-Serie), Voraussetzungen für Präventivmaßnahmen der IT-Sicherheit für Hersteller, Betreiber und Anwender im Gesundheitswesen. Mit der EU-Verordnung 2017/745 über Medizinprodukte (MDR) wird mit Mai 2020 das MPG durch ein weiteres, in der EU abgestimmtes Gesetz, ersetzt werden. Einerseits schützen diese Gesetze die Bürgerinnen und Bürger im digitalen EU-Binnenmarkt, andererseits bieten sie den Herstellern die Grundlagen und die Chancen, ihre Produkte einheitlich auf Safety, Security und Privacy auszurichten.

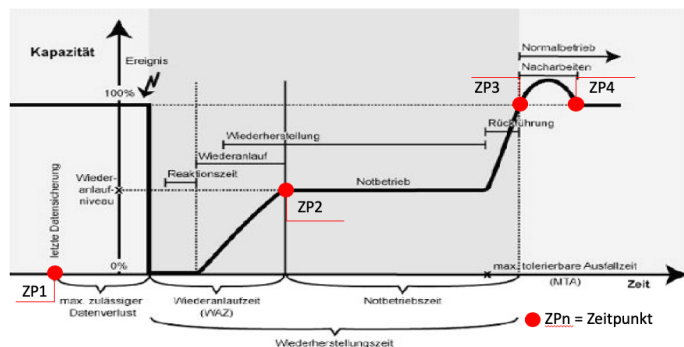
Bei der Anwendung des NISG werden im Sektor Gesundheitswesen nicht alle Krankenhäuser und Privatkliniken in Österreich betroffen sein. Das Gesetz sieht vor, dass die betroffenen Einrichtungen einen Bescheid (siehe NISV §16 Abs. 1) erhalten und dadurch Sicherheitsvorfälle an die NIS-Kontaktstelle melden müssen, wenn ein wesentlicher Dienst für die medizinische Versorgung mehr als drei Stunden ausfällt oder nur eingeschränkt verfügbar ist.

„Im Internet werden unerlaubte freigegebene Labor-Daten von Patientinnen/Patienten gefunden, die/der Datenschutzbeauftragte muss binnen 72 Stunden diesen Data Breach an die DSB<sup>[1]</sup> melden. Bei der Überprüfung dieser IT-Störung wird eine schwerwiegende Fehlfunktion bei der Integrität der Datenergebnisse von Labor-Automaten festgestellt und diese muss unverzüglich an das BASG<sup>[2]</sup> gemeldet werden. Dadurch ist die medizinische Versorgung eingeschränkt und nach 3 Stunden muss an das CERTat<sup>[3]</sup> eine IT-Störung abgegeben werden.“ Die Prozesse für die (IT-)Störfallbehandlungen in der Krankenanstalt habe auf diese 3 Meldewege Rücksicht zu nehmen, um die Koordination der Maßnahmen und die Abstimmung aller Betroffenen bestmöglich zu unterstützen. Es drängt sich die Frage auf: „Ob eine Abstimmung zwischen der DSB, dem BASG und dem Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) auch erfolgt?“ Eine mögliche Erleichterung würde nach Meinung des Autors die Gründung eines HealthCERT beim BASG schaffen, weil sich die Meldungen zum MPG und NISG treffen und die möglicherweise zusammenhängenden IT-Bedrohungen von Safety und Security leichter erkennbar wären.

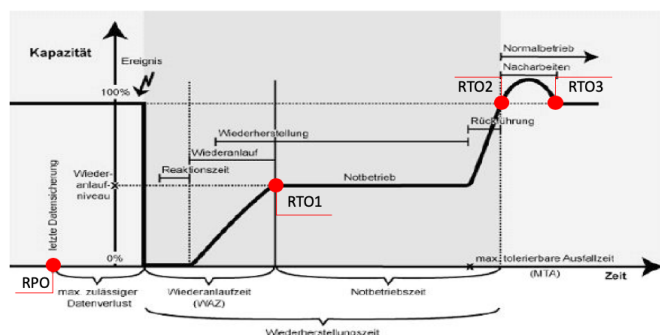
- <sup>[1]</sup> DSB = Datenschutzbehörde – Meldepflicht lt. Art. 33 DSGVO  
<sup>[2]</sup> BASG = Bundesamt für Sicherheit im Gesundheitswesen – Meldepflicht lt. § 70 MPG  
<sup>[3]</sup> CERTat = Computer Emergency Response Team Austria – Meldepflicht lt. § 8 NISV

## RPO / RTO

Recovery POINT Objective &  
 Recovery TIME Objective lt. BSI 100-4



Recovery POINT Objective &  
 Recovery TIME Objective lt. BSI 100-4



RTO1 = Notbetrieb vorhanden

RTO2 = Betrieb + Restore der letzten Datensicherung vorhanden

RTO3 = Betrieb + Restore + Daten nach erfasst

## Risikoanalyse Krankenhaus-IT (Informationstechnik)

Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT (Informationstechnik)

**Achtung:** (Informationstechnik) Die Informationen auf diesen Seiten sind nicht 1:1 auf Österreich anwendbar. Die vorgangsweisen sind aber für Österreich anwenbar.

Krankenhäuser zählen aufgrund ihrer herausragenden Bedeutung für das Wohlergehen und den Schutz der Bevölkerung zu den Kritischen Infrastrukturen unserer Gesellschaft, also zu den Einrichtungen deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen nach sich ziehen würde. Sie haben daher eine besondere Verpflichtung, die Verfügbarkeit ihrer Dienste und der Prozesse, mit denen diese erbracht werden, sicherzustellen.

Diese Broschüre gibt einen kurzen Überblick über die in dem [Leitfaden „Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT \(Informationstechnik\)“](#) dargestellte Methode zur Untersuchung der Risiken, die mit dem zunehmenden Einsatz von Informationstechnik (IT (Informationstechnik)) in einem Krankenhaus verbunden sind. Die Zielsetzungen und der Nutzen dieser – nachfolgend als IT (Informationstechnik)-Risikoanalyse bezeichneten – Methode für die Verbesserung der IT (Informationstechnik)-Sicherheit in einem Krankenhaus werden beschrieben. Darüber hinaus wird gezeigt, wie sich die IT (Informationstechnik)-Risikoanalyse in das übergreifende Risikomanagement eines Krankenhauses einordnen lässt.

Wir führen Risikobewertungen durch, um folgende Fragen beantworten zu können:

Was kann passieren (Gefahr)?

Wodurch kann es passieren (Ursachen, Auslöser)?

Wie schlimm kann es sein (Schadensausmaß)?

Wie wahrscheinlich ist es (Wahrscheinlichkeit)?

Welche Empfehlungen können von der Risikobewertung für das Risikomanagement abgeleitet werden?

Welche Maßnahmen kann das Risikomanagement setzen?

Was bewirken diese Risikomanagement-Maßnahmen?

Würde die Erhebung weiterer Daten die Entscheidung des Risikomanagements beeinflussen?

Würden unrichtige Annahmen die Entscheidung des Risikomanagements ändern? Wenn ja, ist das prüfbar?

Was kostet es, wenn Maßnahmen durchgeführt werden? Was kostet es, wenn keine Maßnahmen durchgeführt werden? Wem entstehen diese Kosten?

Risiko = Auswirkung x Eintrittswahrscheinlichkeit

	gering	← Auswirkungen →	hoch
hoch			
Eintrittswahrscheinlichkeit			
gering			

 [Das österreichische Gesundheitswesen Daten Zahl Fakten - 2019](#)

Die Gesundheitsversorgung in Österreich verfügt über viele Ressourcen.

So liegen etwa die Anzahl der praktizierenden Ärztinnen und Ärzten und das Angebot an Spitalsbetten im Verhältnis zur Bevölkerung im europäischen Spitzenfeld. Generell wird damit ein guter Zugang zum Gesundheitssystem sichergestellt.

Stationäre Versorgung - Prozessschritte

(die Angaben aus Deutschland sind in Österreich vergleichbar)



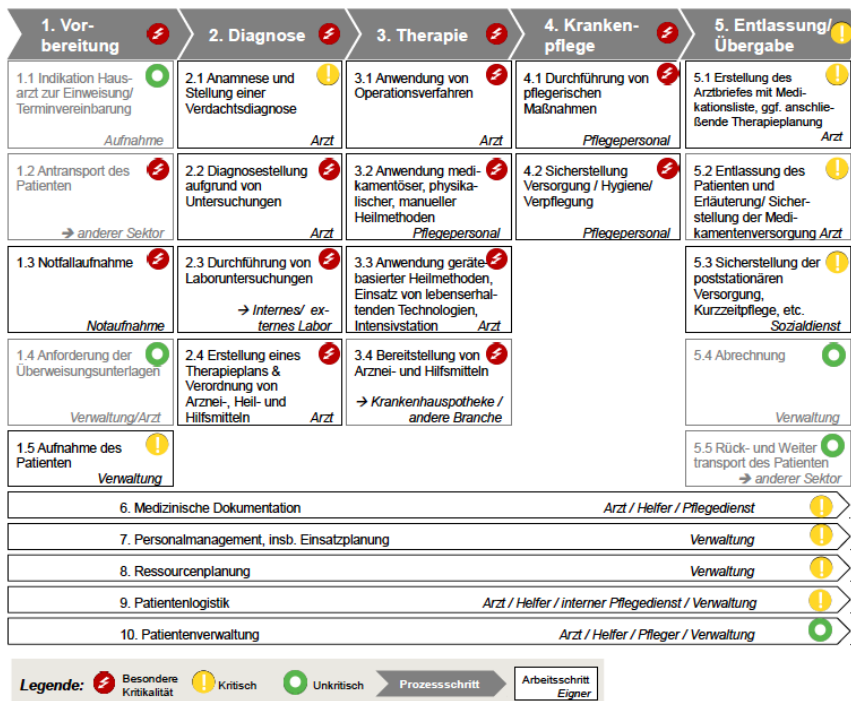


Abbildung 36: Prozess- und Arbeitsschritte (AS) in der stationären Versorgung

## Ambulante Versorgung - Prozessschritte

(die Angaben aus Deutschland sind in Österreich vergleichbar)

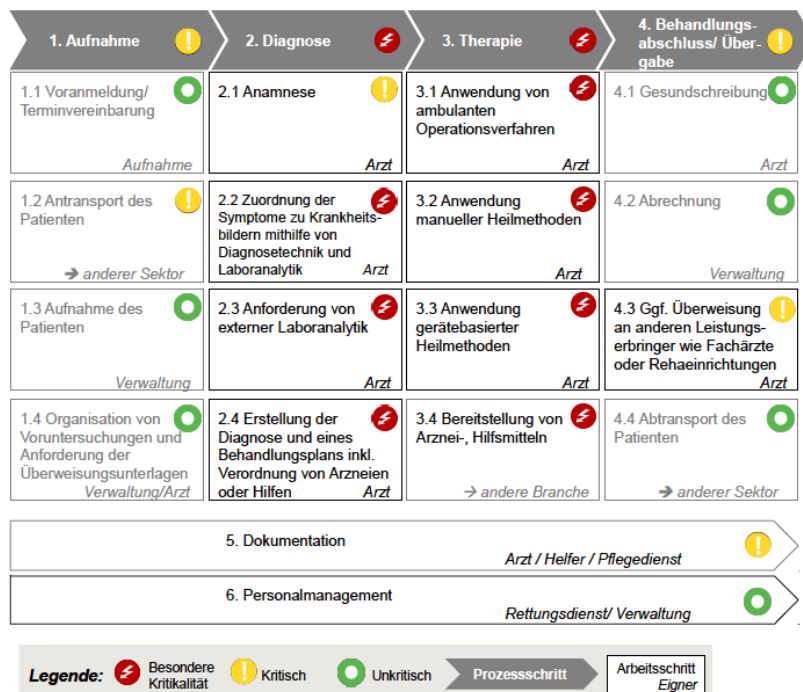
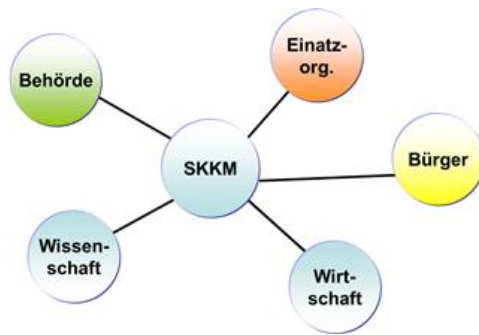


Abbildung 37: Prozess- und Arbeitsschritte bei der ambulanten Versorgung

## Zivilschutz in Österreich

### Staatliches Krisen- und Katastrophenschutzmanagement (SKKM)



Hauptakteure im österreichischen Katastrophenmanagement © Siegfried Jachs, BMI

Die Abwehr, Beseitigung oder Linderung der Auswirkungen drohender oder eingetretener Katastrophen (Katastrophenhilfe, Einsatzvorsorgen) ist in Österreich überwiegend eine Angelegenheit der Bundesländer. Die rechtliche Basis bilden die Katastrophenhilfegesetze der Länder, die vor allem die Feststellung der Katastrophe und die behördliche Einsatzleitung in den Gemeinden, Bezirken und Ländern festlegen.

Bei Krisen und Katastrophen besteht erhöhter Koordinationsbedarf, der in Österreich durch das SKKM gewährleistet wird. Die Geschäftsstelle ist im BMI angesiedelt. Das SKKM ermöglicht eine effiziente Katastrophenhilfe im In- und Ausland, durch die Zusammenarbeit aller zuständigen Stellen des Bundes mit den Katastrophenschutzbehörden der Länder sowie den Hilfs- und Rettungsorganisationen.

Quelle: BMI Krisen- und Katastrophenmanagement



[SKKM - Führen im Katastropheneinsatz in Österreich \(verkürzt\)](#)

## Österreichisches Programm zum Schutz kritischer Infrastrukturen (APCIP)

Das österreichische Programm zum Schutz kritischer Infrastrukturen (Austrian Program for Critical Infrastructure Protection - APCIP) beschreibt den strategischen und konzeptuellen Rahmen, die Prinzipien und strategischen Zielsetzungen und die Handlungsfelder und Maßnahmen zum Schutz kritischer Infrastruktur.

Kritische Infrastrukturen sind nach APCIP: „*Kritische Infrastrukturen im Sinne dieses Masterplans sind jene Infrastrukturen (Systeme, Anlagen, Prozesse, Netzwerke oder Teile davon), die eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben und deren Störung oder Zerstörung schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung oder das effektive Funktionieren von staatlichen Einrichtungen haben würde.*“

Der Masterplan APCIP nutzt als Grundlage die Prinzipien Kooperation, Subsidiarität, Komplementarität, Vertraulichkeit und Verhältnismäßigkeit und basiert auf einem All-hazards-Ansatz. (Unter dem All-Hazards-Ansatz wird ein Ansatz verstanden, der im Rahmender Sicherheitsvorsorge das gesamte Spektrum der potenziellen Bedrohungen umfasst.) Der Fokus des Masterplans ist die Unterstützung von strategischen Unternehmen beim Aufbau einer umfassenden Sicherheitsarchitektur (Risikomanagement, Business Continuity Management und Sicherheitsmanagement).

Das Programm soll langfristig zur Steigerung der Resilienz und Sicherheit in Österreich beitragen. Resilienz wird in APCIP beschrieben als: „*die Fähigkeit eines Systems, einer Gemeinschaft oder einer Gesellschaft, welche(s) Gefahren ausgesetzt ist, deren Folgen zeitgerecht und wirkungsvoll zu bewältigen, mit ihnen umzugehen, sich ihnen anzupassen und sich von ihnen zu erholen, auch durch Bewahrung und Wiederherstellung seiner bzw. ihrer wesentlichen Grundstrukturen und Funktionen.*“

## Traffic Light Protocol (TLP)

Das Ampelprotokoll wurde geschaffen, um das Teilen sensibler Informationen zwischen Organisationen zu fördern. Der Absender muss signalisieren, inwieweit seine Informationen über den unmittelbaren Empfänger hinaus weitergegeben werden sollen, wenn überhaupt.

Das Ampelprotokoll basiert auf dem Konzept, dass der Absender Informationen mit einer von vier Farben kennzeichnet, um anzugeben, inwiefern die Informationen durch den Empfänger weitergegeben werden können. Der Empfänger muss den Absender konsultieren, wenn eine Weitergabe erforderlich ist.

**Die vier Farben und ihre Bedeutung sind wie folgt:**

**ROT** – Privat und nur für die genannten Empfänger bestimmt. Im Rahmen einer Besprechung zum Beispiel sind rot gekennzeichnete Informationen auf die Anwesenden beschränkt. In den meisten Fällen werden die rot gekennzeichneten Informationen mündlich oder persönlich weitergegeben.

**GELB** – Begrenzte Weitergabe. Der Empfänger darf gelb gekennzeichnete Informationen an andere Personen in seiner Organisation weitergeben, allerdings nur, wenn diese unbedingt in Kenntnis gesetzt werden müssen. Es wird möglicherweise vom Absender erwartet, dass er die Grenzen der Weitergabe angibt.

**GRÜN** – Für die gesamte Gemeinschaft. Informationen in dieser Kategorie können innerhalb einer bestimmten Gemeinschaft weitergegeben werden. Die Informationen dürfen jedoch weder im Internet noch anderweitig veröffentlicht oder außerhalb der Gemeinschaft preisgegeben werden.

**WEISS** – Unbegrenzt. Vorbehaltlich der üblichen Urheberrechtsbestimmungen dürfen weiß gekennzeichnete Informationen frei und ohne Einschränkung weitergegeben werden.

Sensible Informationen, wie auch immer sie von einem Absender bereitgestellt werden, sollten zum Zeitpunkt der Offenlegung in Übereinstimmung mit dem Ampelprotokoll gekennzeichnet sein. Alle sensiblen Informationen gelten als mit gelber Kennzeichnung versehen, sofern nichts anderes angegeben oder schriftlich mitgeteilt wird. Standardmäßig und sofern zum Zeitpunkt der Offenlegung keine anderslautenden Festlegungen bestehen, wird die Identität der Quelle der sensiblen Informationen jedoch immer rot gekennzeichnet sein.

---

## Fernunterricht - Teams / Aufgaben

### Risikomanagement für medizinische IKT-Netzwerke

Im Krankenhaus sind INTERNE PARTNER, wie die IKT-Abteilung (Informations- und Kommunikationstechnik), die Medizintechnik, die Haustechnik, die Abteilung Einkauf und/oder der Risikomanager, für das Risikomanagement in medizinischen IKT-Netzwerken verantwortlich. EXTERNE PARTNER, wie die Medizinprodukte-Hersteller und mögliche Dienstleister, sollten (müssen) diesen Prozess unterstützen.

Die Komplexität in medizinischen IKT-Netzwerken ist von vielen Faktoren abhängig:

die Zweckbestimmung des Medizinproduktes (definiert der Hersteller)

die Komplexität z.B.:

vernetzte Medizinprodukte

IKT-Systeme und IKT-Netzwerkinfrastruktur

Technische Abhängigkeiten und Schnittstellen

Systemdesign durch den Hersteller des Medizinproduktes

Durchmischung von Medizinprodukten, IKT-Systeme und IKT-Netzwerke (Betreiber & Hersteller)

uvm.

### Modellierung von ereignisorientierten Prozessketten (EPK)

#### **Abfolge von Ereignissen und Funktionen in Prozessketten**

Die EPK beginnt mit einem Start-/Auslöseereignis und endet mit dem End-/Ergebnisereignis oder mit einem Prozesswegweiser. Zwischen Start- und Endereignis lösen sich Ereignisse und Funktionen ab. Es können nicht zwei Funktionen oder zwei Ereignisse aufeinanderfolgen. Möglich ist allerdings, dass Funktionen bzw. Ereignisse parallel angeordnet werden können. Für diese Darstellung werden die logischen Operatoren benötigt. Die Verbindung zwischen Ereignis und Funktion erfolgt durch eine Pfeillinie.

---

## MIS Extramural

### Mitarbeit WS

Mitarbeitsplus werden am Ende der Stunde eingetragen, bitte diese einfordern!

### Mitarbeit SS

---

## E1 FHIR Server

Todo: erstellen eines Portfolio Ordners für MIS mit

Unterlagen

Ausarbeitungen

Abgaben

Projektverzeichnis

Unterlagen sind bei der Matura erlaubt (100 MiB Ordner gesammelt für die ges. Klasse => laufend erstellen)

Was haben wir bisher umgesetzt? => Erstellen eines Basisprojekts mit

Practitioner,

Patient,

Encounter

 [E1 Lab1 Basisprojekt mit Practitioner, Patient und Encounter](#)

Umsetzung von reservierten Wörtern in Java Enums:

```
public enum StatusCode {
    planned("planned"),
    arrived("arrived"),
    triaged("triaged"),
    inprogress("in-progress"), // - wäre in Java nicht erlaubt, so funktioniert es
    onleave("onleave"),
    finished("finished"),
    cancelled("cancelled");

    private String value;
    private StatusCode(String value)
    {
        this.value = value;
    }

    public String toString()
    {
        return this.value;
    }
}
```










 [E1 Lab 2: Umsetzung der Medication](#)

Wir können bisher noch keine Medikationsdaten speichern.

Das ist natürlich schade, nachdem Medikamente ein wichtiger Teil der Gesundheitsbranche darstellen.

In FHIR gibt es ein Datenmodell, das wir umsetzen können:

<https://hl7.org/FHIR/medication.html>

Name	FlagsCard.Type		Description & Constraints ?
 <a href="#">Medication</a>	TU	<a href="#">DomainResource</a>	Definition of a Medication Elements defined in Ancestors: <a href="#">id</a> , <a href="#">meta</a> , <a href="#">implicitRules</a> , <a href="#">language</a> , <a href="#">text</a> , <a href="#">contained</a> , <a href="#">extension</a> , <a href="#">modifierExtension</a>
 <a href="#">identifier</a>	Σ	0..* <a href="#">Identifier</a>	Business identifier for this medication
 <a href="#">code</a>	Σ	0..1 <a href="#">CodeableConcept</a>	Codes that identify this medication <a href="#">SNOMED CT Medication Codes (Example)</a>
 <a href="#">status</a>	?!Σ	0..1 <a href="#">code</a>	active   inactive   entered-in-error <a href="#">Medication status codes (Required)</a>
 <a href="#">manufacturer</a>	Σ	0..1 <a href="#">Reference(Organization)</a>	Manufacturer of the item
 <a href="#">form</a>		0..1 <a href="#">CodeableConcept</a>	powder   tablets   capsule + <a href="#">SNOMED CT Form Codes (Example)</a>
 <a href="#">amount</a>	Σ	0..1 <a href="#">Ratio</a>	Amount of drug in package
 <a href="#">ingredient</a>		0..* <a href="#">BackboneElement</a>	Active or inactive ingredient
 <a href="#">item[x]</a>		1..1	The actual ingredient or content

itemCodeableConcept		<a href="#"><u>CodeableConcept</u></a>	
itemReference		<a href="#"><u>Reference(</u></a> <a href="#"><u>Substance</u></a> <a href="#"><u> </u></a> <a href="#"><u>Medication</u></a> <a href="#"><u>)</u></a>	
isActive	0..1	<a href="#"><u>boolean</u></a>	Active ingredient indicator
strength	0..1	<a href="#"><u>Ratio</u></a>	Quantity of ingredient present
batch	0..1	<a href="#"><u>BackboneElement</u></a>	Details about packaged medications
lotNumber	0..1	<a href="#"><u>string</u></a>	Identifier assigned to batch
expirationDate	0..1	<a href="#"><u>dateTime</u></a>	When batch will expire

Setze diese FHIR Ressource in unserem Projekt um. Es sind Controller, Tests, Testdaten in der import.sql und Repositories ebenfalls gefragt!

### [E1 Lab 3: Recherche e-Medikation und FHIR Medication](#)

In Österreich gibt es mit der e-Medikation eine Lösung, um Medikamente elektronisch zu verschreiben.

Der FHIR Standard ist jedoch international und wird nicht genau zu der e-Medikation passen.

Starte eine Suche und recherchiere, welche Datenfelder in der e-Medikation vorkommen und was der Unterschied zur FHIR Medication ist.

Können wir die e-Medikation in unserem FHIR Modell speichern? Welche Änderungen wären notwendig?

Erstelle ein Dokument, das diese Fragen beantwortet. Falls du auf <https://www.chipkarte.at/cdscontent/?contentid=10007.678631&portal=ecardportal> Informationen suchst, dann ist das Passwort dafür "arztsoftware".

### [GitHub Musterlösung](#)

## [E2 Angular Client](#)

Wir haben bisher von unserem APIS den Server umgesetzt. Wir können Daten speichern und im FHIR Format über eine REST Schnittstelle anbieten.

Diese REST Schnittstelle können wir nutzen. Wir bauen einen Client, der die Daten anzeigen kann.

Möglich wären alle Arten von Clients, Web- Mobile- und sogar Desktopclients, die alle auf unser Webservice zugreifen können.

Wir wählen einen Webclient mit Angular. Was ist Angular? Wir werden es kennenlernen 😊

Unterlagen:

Eine Sammlung an Tools/Ressourcen rund um Angular: <https://angular.io/resources>

### [2 Typescript Intro](#)

### [Angular CheatSheet](#)

### [angular-from-theory-to-practice](#)

### [Typescript Quick Guide](#)

### [Typescript für Java/C# Entwickler](#)

### [Übung Typescript:](#)

















### [Typescript Online Editor](#)

Installation von Angular für den Client





### [Einrichtung Angular Entwicklungsumgebung](#)

### [Empfohlen: Playground for UI Design](#)

### [Empfohlen: Chrome Plugin for debugging](#)

-  [Empfohlen: Angular Material](#)
-  [Angular Project Structure](#)
-  [Stundenwiederholung Angular](#)
-  [E2 Lab1: Erste Aufgabe](#)
-  [Presentation1: Vue vs React vs Angular CLIL](#)
-  [Lab2 User Details REST](#)
-  [E2 Lab2 User Details + Erweiterung](#)
-  [Anleitung Patientenliste](#)
-  [Anleitung Patientendetails](#)
-  [Aufgabe Practitioner - Liste & Details](#)
-  [Anleitung Patient editieren](#)
-  [Aufgabe Practitioner - editieren](#)
-  [Hilfestellung Flag: Reference Links im Client umsetzen](#)
-  [Aufgabe: Verbesserung MÜ 1 2 \(Abgabegespräch\)](#)
-  [MIS 4 8 Lab2 Patient](#)
-  [MIS 4 8 Lab3 Patient Tests](#)












## E3 Maturavorbereitung

-  [Unterlagensammlung 1 Sammlung pro Klasse, max 100Mib](#)
-  [Infos zur Matura](#)
-  [Fragensammlung zur Matura \(extramural\)](#)
-  [Übungsaufgabe + Abgabegespräch](#)

Diese Aufgabe ist ähnlich aufgebaut, wie die schriftliche Matura und sollte als Probe in ~2,5h bewältigt werden können.



Wichtig: Bei der Matura seid ihr offline, also arbeitet jetzt auch komplett offline, so seht ihr, ob der Unterlagenordner vollständig und brauchbar ist.

Die umzusetzende Ressource ist PractitionerRole:

 <a href="#">PractitionerRole</a>	<a href="#">TU</a>	<a href="#">DomainResource</a>	Roles/organizations the practitioner is associated with
			Elements defined in Ancestors: <a href="#">id</a> , <a href="#">meta</a> , <a href="#">implicitRules</a> , <a href="#">language</a> , <a href="#">text</a> , <a href="#">contained</a> , <a href="#">extension</a> , <a href="#">modifierExtension</a>
 <a href="#">identifier</a>	<a href="#">Σ</a>	0..* <a href="#">Identifier</a>	Business Identifiers that are specific to a role/location
 <a href="#">active</a>	<a href="#">Σ</a>	0..1 <a href="#">boolean</a>	Whether this practitioner role record is in active use
 <a href="#">period</a>	<a href="#">Σ</a>	0..1 <a href="#">Period</a>	The period during which the practitioner is authorized to perform in these role(s)
 <a href="#">practitioner</a>	<a href="#">Σ</a>	0..1 <a href="#">Reference(Practitioner)</a>	Practitioner that is able to provide the defined services for the organization
 <a href="#">specialty</a>	<a href="#">Σ</a>	0..* <a href="#">CodeableConcept</a>	Specific specialty of the practitioner
 <a href="#">availableTime</a>		0..* <a href="#">BackboneElement</a>	Times the Service Site is available
 <a href="#">daysOfWeek</a>		0..* <a href="#">code</a>	mon   tue   wed   thu   fri   sat   sun
 <a href="#">allDay</a>		0..1 <a href="#">boolean</a>	Always available? e.g. 24 hour service
 <a href="#">availableStartTime</a>		0..1 <a href="#">time</a>	Opening time of day (ignored if allDay = true)
 <a href="#">availableEndTime</a>		0..1 <a href="#">time</a>	Closing time of day (ignored if allDay = true)

In der Speciality sind folgende 2 Codes zu ermöglichen:

System URL: <http://snomed.info/sct>  <https://www.hl7.org/fhir/external.png>

Code	Display
<a href="https://www.hl7.org/fhir/external.png">408467006</a> 	Adult mental illness
<a href="https://www.hl7.org/fhir/external.png">394577000</a> 	Anesthetics

Beide dieser Felder sind bei den Tests zu verwenden.

Wichtig: Wenn benötigte Informationen nicht vorhanden sind, dann sind sinnvolle Annahmen zu treffen und in einem Kommentar zu vermerken.

1. Erstelle das Model so, dass die Tabellen erzeugt werden und gibt das über Reverse Engineering erzeugte ER Datenmodell ab (5 Punkte)
2. Erstelle ein Repository, einen Controller, UnitTests und Testdatensätze im import.sql (5 Punkte)
3. Erstellen des Clients mit einer Liste an PractitionerRoles, einer Detailansicht für eine PractitionerRole mit allen Identifiern, der Period mit start und end, availableEndTime jeweils editier-, speicher-, und löschar. Dazu gehören dieComponents, Modelklassen und Services.(5 Punkte)
4. Theoriefragen, (5 Punkte) z.B.


Die Gruppenpraxis ist über die Entwicklung erfreut, hat jedoch ein paar Anfragen zur Beantwortung an Sie gestellt.

- a) Eine der Praxen hat noch eine alte Datenbank, dessen Schema nicht dem FHIR Standard entspricht. Es soll das System jedoch FHIR unterstützen. Muss das Datenbankschema diesem Standard entsprechen? Welche Lösung schlagen Sie vor?
- b) Wieso ist in dem Projekt von MEDIKOM kein SQL Code zu finden? Wie funktioniert der Datenbankzugriff ohne SQL?

Viel Spaß bei der Umsetzung!

---

## Maturavorbereitung INTRAMURAL

 [BSI - IT-Grundschutz- Kompendium 2020 / NEU mit 07. Mai 2020](#)

Bitte sehen Sie sich dieses IT-Grundschutz-Kompendium 1x an, viele Punkte können Ihnen bei der Ausarbeitung helfen.

Sie sollen die Vorschläge aber immer an die Aufgabenstellung anpassen. Eine 1:1 Kopie ist daher nicht Sinnvoll.

mit freundlichen Grüßen

F. Hoheiser-Pförtner

Ps: Dieses Dokument wird noch in die Informationssammlung aufgenommen

---

## Thema 13

Sie sind angemeldet als Elshazly Salma (Logout)

Startseite

Unsere Datenlöschfristen

Laden Sie die mobile App

# MIS - Medizinische Informationssysteme - 5BHBGM - SJ2021

[Startseite](#) / [Meine Kurse](#) / [HBGM](#) / [5BHBGM](#) / [MIS 5BHBGM 2021](#) / [Beurteilung von Richtlinien: RICHTIG oder FALSCH?](#)  
/ [Richtlinie für KRITIKALITÄTSANALYSE:](#)

## Richtlinie für KRITIKALITÄTSANALYSE:

*Bei der Kritikalitätsanalyse werden aus der Prozessübersicht des SPITALS diejenigen Prozesse ausgewählt, deren Ausfall oder Störung zu schwerwiegenden Verletzungen der Schutzziele der Gesundheitseinrichtung führen würden.*

**Diese Prozesse werden als kritische Prozesse bezeichnet.**

*Zur Auswahl der kritischen Prozesse sind folgende Kriterien entscheidend:*

1. die Auswirkungen eines Prozessausfalls auf Leben und Gesundheit,
2. der Umfang eines Prozessausfalls,
3. die gesetzliche, vertragliche oder gesellschaftspolitische Relevanz der Ausfallsfolgen und dabei
  - 3a. die potenziellen Auswirkungen der Verletzung der Vertraulichkeit von personenbezogenen Daten für die betroffene Person,
  - 3b. die Ausfallszeit (Minuten, Stunden, Tage), an dem die Auswirkungen eines Ausfalls als kritisch anzusehen ist,
4. die mit einem Ausfall verbundenen wirtschaftlichen Schäden.

*Bei der Kritikalitätsanalyse werden Bedrohungen ermittelt, die die Prozesse nach den oben angeführten Kriterien beeinflussen.*

1. Warum ist diese Richtlinie **RICHTIG** ist oder **FALSCH**.
2. Warum ist z.B. die Bedrohung "RANSOMWARE" als kritisch, für einen Prozesse in der Gesundheitsversorgung im Spital zu bewerten.



- Diese Richtlinie ist RICHTIG, weil die IKT-Systeme/Anwendungen und/oder das IKT-Netzwerk, die für kritischen Prozesse verwendet werden, durch definierte Vorgangsweise behandelt werden.

Die Vorgangsweise für die Bewertung könnte mit folgender Frage überprüft werden.

**Frage:** Sind die IKT-Systeme und das IKT-Netzwerk des Prozesses durch die Bedrohung der CIA-Triade gefährdet?

- JA, wir haben Schutzmaßnahmen gegen den Verlust der Vertraulichkeit und der Integrität getroffen.
- JA, wir haben auch Redundanzen für die IKT-Systeme/Anwendungen und das IKT-Netzwerk eingesetzt.
- Damit wir die Ordnungsmäßigkeit dieser Maßnahmen nachweisen können, werden diese permanent überwacht (Monitoring). Ist die permanente Überwachung nicht möglich, dann überprüfen wird regelmäßig abhängig von der Kritikalität des Prozesses durch Pen-Test 1 x am Tag, Woche, Monate, Halbjahr und Jahr.
- Vor Einsatz oder Änderung des IKT-Systems/Anwendung und/oder des IKT-Netzwerks werden definierte Abnahmeprüfungen durchgeführt.
- Beim Monitoring oder Pen-Testen ist genau definiert, WER, WIE und nach welcher ZEIT informiert wird (Meldeweg). Hierbei ist auch festgelegt, welche Eskalationen nach welcher ZEIT durchgeführt werden.
- Durch die Kritikalität der Prozesse ist auch die Vorgangsweise im Katastrophenfall (K-Fall) definiert. Wir haben eine eigene Katastrophenstruktur in der IKT definiert oder können auch in die Katastrophenstruktur im Spital eingebunden werden.
- Die Bedrohung "RANSOMWARE" ist für die Prozesse im Spital KRITISCH, weil durch die Verschlüsselung der Daten katastrophale Folgen bei der Versorgung der Patientinnen und Patienten entstehen können. Daher werden Maßnahmen getroffen, wie sie oben beschrieben sind. Ein weiterer Punkt ist das IKT-Security-Awareness-Training für das Personal und andere Personen im Spital.

◀ Falsche Maßnahmen oder Fehler der Personen

Direkt zu:

Dokumentenlenkung Beschreibung ►

Sie sind angemeldet als Zawislak Konrad (Logout)  
MIS\_5BHBGM\_2021

Unsere Datenlöschfristen  
Laden Sie die mobile App

# MIS - Medizinische Informationssysteme - 5BHBGM - SJ2021

[Startseite](#) / [Meine Kurse](#) / [HBGM](#) / [5BHBGM](#) / [MIS 5BHBGM 2021](#) / [Netz- und Informationssystemsicherheitsgesetz - Ri...](#)  
/ [Prozesse für \(IT-\)Störfallbehandlungen werden imme...](#)

## Prozesse für (IT-)Störfallbehandlungen werden immer WICHTIGER!

*Der Gesetzgeber hat seit vielen Jahren Safety und Security im Gesundheitssektor in verschiedenen Gesetzen verankert, wie z. B. dem Gesundheitstelematikgesetz 2012 (GTeIG 2012), dem Medizinproduktegesetz (MPG) sowie seit 2018 in der Datenschutzgrundverordnung (DSGVO) und im Netz- und Informationssystemsicherheitsgesetz (NISG). Besonders „Security & Privacy by Design & Default“ sind, neben den Abstimmungen der involvierten Personen (z. B. anhand der ISO/IEC 27000-Serie und/oder der ISO/IEC 80001-Serie), Voraussetzungen für Präventivmaßnahmen der IT-Sicherheit für Hersteller, Betreiber und Anwender im Gesundheitswesen. Mit der EU-Verordnung 2017/745 über Medizinprodukte (MDR) wird mit Mai 2020 das MPG durch ein weiteres, in der EU abgestimmtes Gesetz, ersetzt werden. Einerseits schützen diese Gesetze die Bürgerinnen und Bürger im digitalen EU-Binnenmarkt, andererseits bieten sie den Herstellern die Grundlagen und die Chancen, ihre Produkte einheitlich auf Safety, Security und Privacy auszurichten.*

*Bei der Anwendung des NISG werden im Sektor Gesundheitswesen nicht alle Krankenhäuser und Privatkliniken in Österreich betroffen sein. Das Gesetz sieht vor, dass die betroffenen Einrichtungen einen Bescheid (siehe NISV §16 Abs. 1) erhalten und dadurch Sicherheitsvorfälle an die NIS-Kontaktstelle melden müssen, wenn ein wesentlicher Dienst für die medizinische Versorgung mehr als drei Stunden ausfällt oder nur eingeschränkt verfügbar ist.*

*„Im Internet werden unerlaubte freigegebene Labor-Daten von Patientinnen/Patienten gefunden, die/der Datenschutzbeauftragte muss binnen 72 Stunden diesen Data Breach an die DSB<sup>[1]</sup> melden. Bei der Überprüfung dieser IT-Störung wird eine schwerwiegende Fehlfunktion bei der Integrität der Datenergebnisse von Labor-Automaten festgestellt und diese muss unverzüglich an das BASG<sup>[2]</sup> gemeldet werden. Dadurch ist die medizinische Versorgung eingeschränkt und nach 3 Stunden muss an das CERTat<sup>[3]</sup> eine IT-Störung abgegeben werden.“ Die Prozesse für die (IT-)Störfallbehandlungen in der Krankenanstalt habe auf diese 3 Meldewege Rücksicht zu nehmen, um die Koordination der Maßnahmen und die Abstimmung aller Betroffenen bestmöglich zu unterstützen. Es drängt sich die Frage auf: „Ob eine Abstimmung zwischen der DSB, dem BASG und dem Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) auch erfolgt?“ **Eine mögliche Erleichterung würde nach Meinung des Autors die Gründung eines HealthCERT beim BASG schaffen, weil sich die Meldungen zum MPG und NISG treffen und die möglicherweise zusammenhängenden IT-Bedrohungen von Safety und Security leichter erkennbar wären.***

<sup>[1]</sup> DSB = Datenschutzbehörde – Meldepflicht lt. Art. 33 DSGVO

<sup>[2]</sup> BASG = Bundesamt für Sicherheit im Gesundheitswesen – Meldepflicht lt. § 70 MPG

<sup>[3]</sup> CERTat = Computer Emergency Response Team Austria – Meldepflicht lt. § 8 NISV

Zuletzt geändert: Wednesday, 6. November 2019, 18:15

◀ [Dokumentenlenkung Beschreibung](#)

Direkt zu:

[Das österreichische Gesundheitswesen Daten Zahl Fakten - 2019 ▶](#)

Sie sind angemeldet als Zawislak Konrad (Logout)  
MIS\_5BHBGM\_2021

Unsere Datenlöschfristen  
[Laden Sie die mobile App](#)



# MIS - Medizinische Informationssysteme - 5BHBGM - SJ2021

[Startseite](#) / [Meine Kurse](#) / [HBGM](#) / [5BHBGM](#) / [MIS 5BHBGM 2021](#) / [Fernunterricht - Teams / Aufgaben](#)  
/ [Risikomanagement für medizinische IKT-Netzwerke](#)

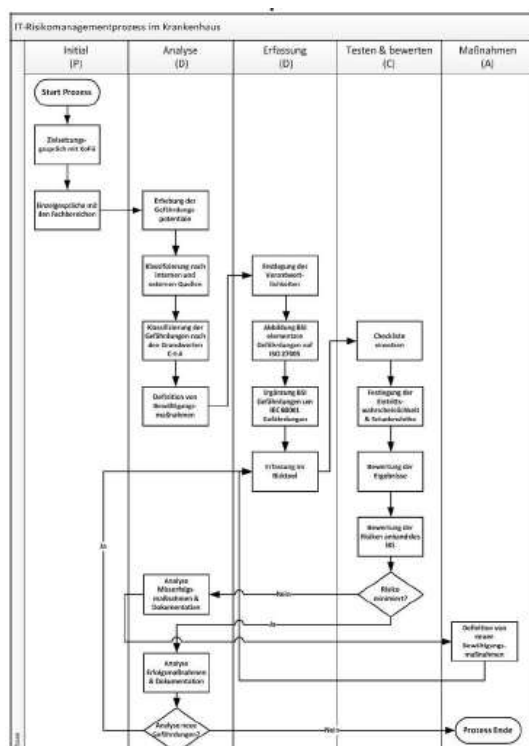
## Risikomanagement für medizinische IKT-Netzwerke

Im Krankenhaus sind INTERNE PARTNER, wie die IKT-Abteilung (Informations- und Kommunikationstechnik), die Medizintechnik, die Haustechnik, die Abteilung Einkauf und/oder der Risikomanager, für das Risikomanagement in medizinischen IKT-Netzwerken verantwortlich. EXTERNE PARTNER, wie die Medizinprodukte-Hersteller und mögliche Dienstleister, sollten (müssen) diesen Prozess unterstützen.

Die Komplexität in medizinischen IKT-Netzwerken ist von vielen Faktoren abhängig:

- die Zweckbestimmung des Medizinproduktes (definiert der Hersteller)
- die Komplexität z.B.:
  - vernetzte Medizinprodukte
  - IKT-Systeme und IKT-Netzwerkinfrastruktur
  - Technische Abhängigkeiten und Schnittstellen
  - Systemdesign durch den Hersteller des Medizinproduktes
  - Durchmischung von Medizinprodukten, IKT-Systeme und IKT-Netzwerke (Betreiber & Hersteller)
  - uvm.

Der PDCA-Risiko-Prozess könnte wie folgt ablaufen:



Zuletzt geändert: Monday, 23. March 2020, 09:34

◄ SKKM - Führen im Katastropheneinsatz in Österreich (verkürzt)

Direkt zu:

Modellierung von ereignisorientierten Prozessketten (EPK) ►

Sie sind angemeldet als Zawislak Konrad (Logout)

MIS\_5BHBGM\_2021

[Unsere Datenlöschfristen](#)

[Laden Sie die mobile App](#)