VORARLBERGER
LANDESKRANKENHÄUSER

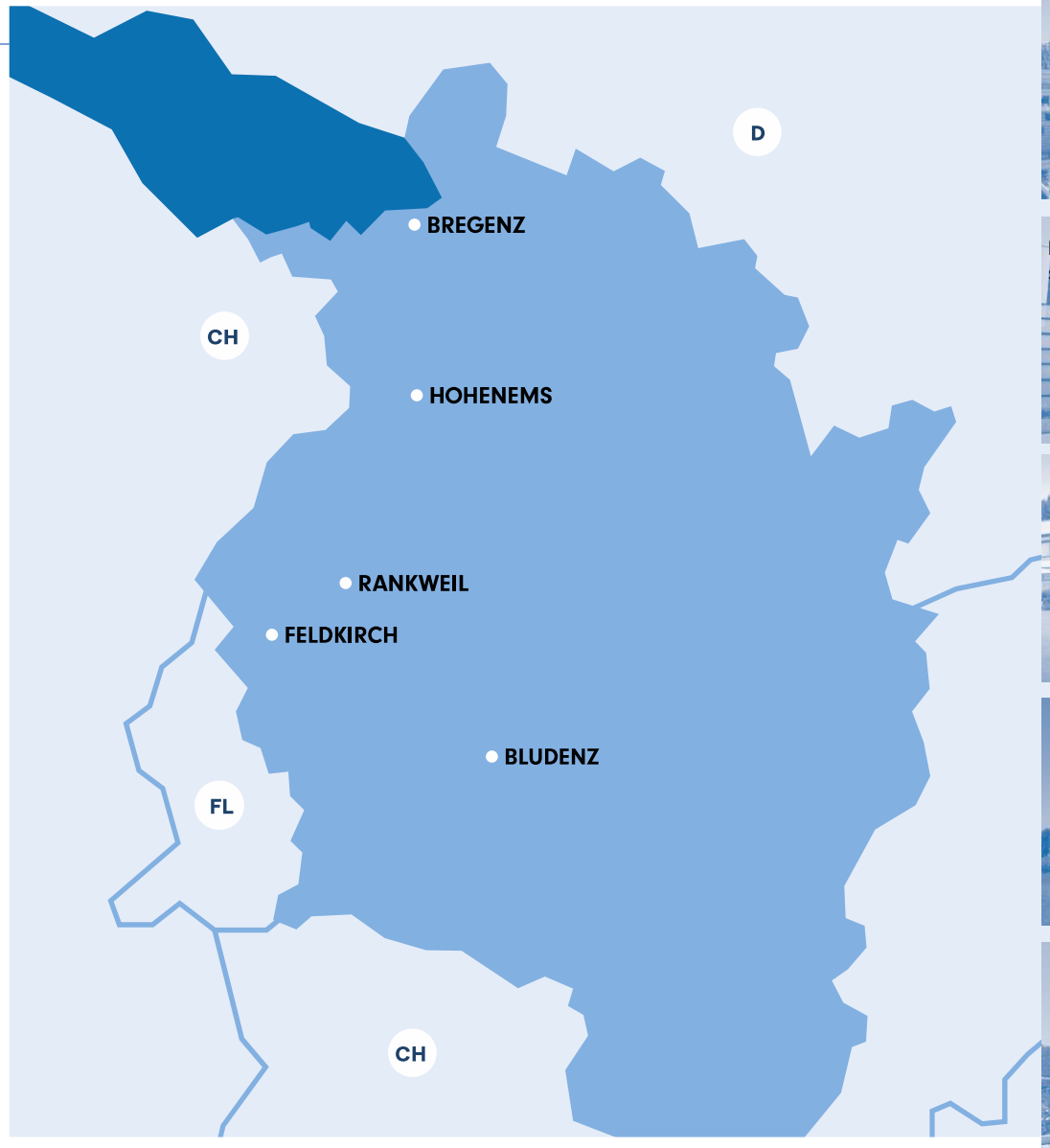
23. April 2024

Vorarlberger
Landeskrankenhäuser

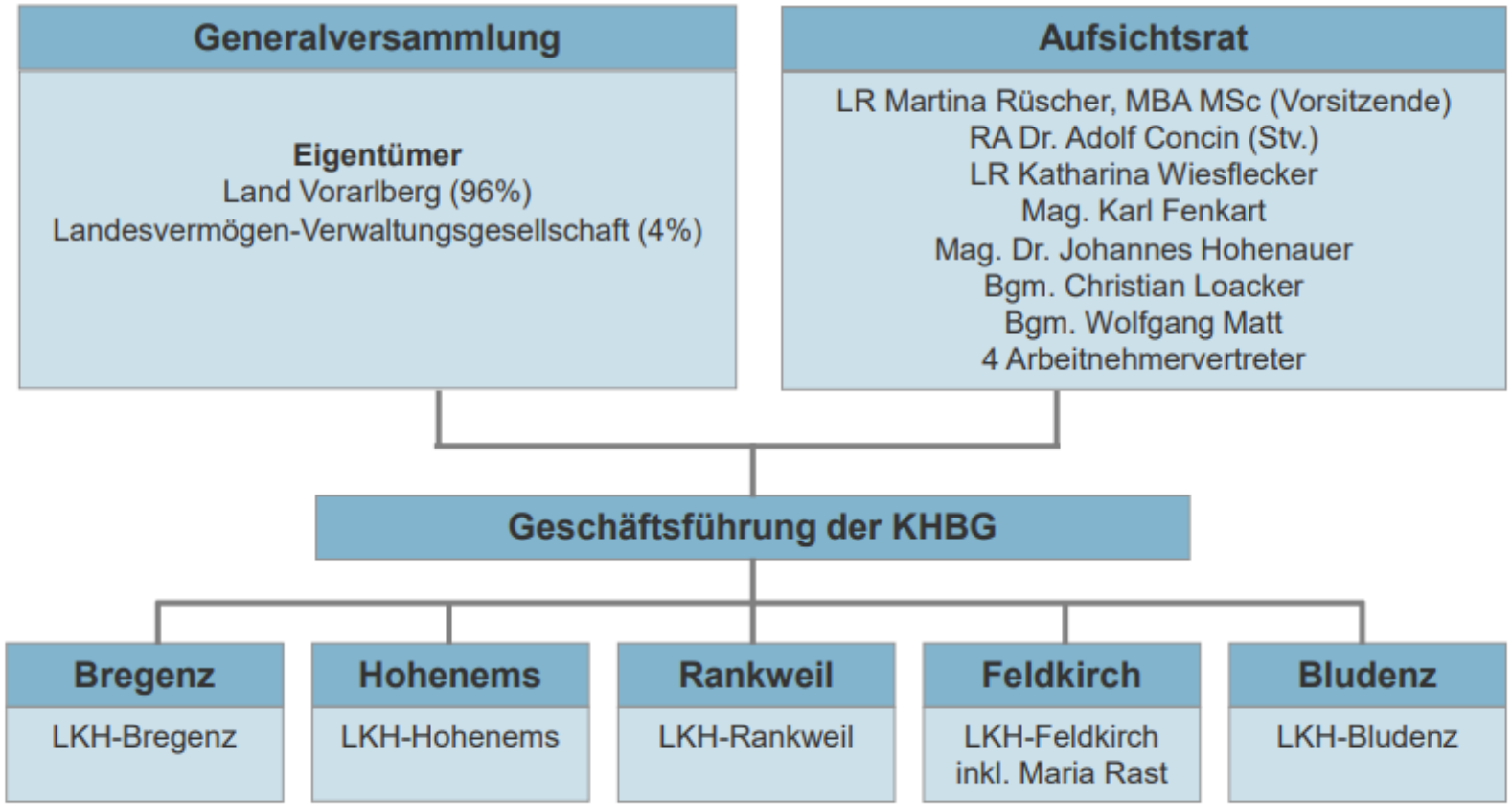
Die Vorarlberger Landeskrankenhäuser
Das Unternehmen

5 Landeskrankenhäuser

Tochterunternehmen/Beteiligungen:
- AZGV (Ausbildungszentrum Gesundheit Vorarlberg – Pflegeschule)
- MPAV (Med.-Produkte-Aufbereitung Vlbg.)
- CSV (Clinic Service Vorarlberg)



Organigramm der Vorarlberger Landeskrankenhäuser



www.landeskrankenhaus.at

Die Vorarlberger Landeskrankenhäuser
Das Unternehmen (Stand 2022)

- 1.522 Betten an 5 Standorten
- 77.900 stationäre Fälle pro Jahr, davon
- 460.000 ambulante Frequenzen pro Jahr
- 2.800 Geburten
- 43.700 Operationen
- 4.710 Mitarbeiter:innen davon 72% weiblich
- 858 Ärzt:innen
- 2.232 Pflegekräfte
- Umsatzvolumen: ca. 610 Mio. € pro Jahr
- Investitionsvolumen: ca. 50 Mio. € pro Jahr

Die Vorarlberger Landeskrankenhäuser sind sowohl eines der größten Unternehmen, als auch einer der größten Arbeitgeber und Investoren in die heimische Wirtschaft.

KHBG / VLKH und NIS – G

(Erfahrungsbericht)

Netz- und Informationssystemsicherheitsgesetz

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

§ 2. Mit diesem Bundesgesetz werden Maßnahmen festgelegt, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen von Betreibern wesentlicher Dienste in den Sektoren

1. Energie,
2. Verkehr,
3. Bankwesen,
4. Finanzmarktinfrastrukturen,
5. Gesundheitswesen,
6. …..

Gesetz / Bescheid

§ 17 Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste

Absatz 1
Zur Gewährleistung der NIS haben Betreiber wesentlicher Dienste in Hinblick auf die Netz- und Informationssysteme, die sie für die Bereitstellung des wesentlichen Dienstes nutzen, geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen. Diese haben den Stand der Technik zu berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein.

Absatz 3
Die Betreiber wesentlicher Dienste haben mindestens **alle drei Jahre nach Zustellung des Bescheides** gemäß § 16 Abs. 4 Z 1 die Erfüllung der Anforderungen nach Abs. 1 gegenüber dem Bundesminister für Inneres nachzuweisen. Zu diesem Zweck übermitteln sie eine Aufstellung der vorhandenen Sicherheitsvorkehrungen durch den Nachweis von Zertifizierungen oder durchgeführten Überprüfungen **durch qualifizierte Stellen**, …..

Bundeskanzleramt

bundeskanzleramt.gv.at

BKA - I/8 (Cyber Security, GovCERT, NIS-Büro und ZAS)
Mag. Anna-Katharina BACHOFNER
Sachbearbeiterin

Anna.Bachofner@bka.gv.at
+43 1 53 115-202732
Ballhausplatz 2, 1010 Wien

E-Mail-Antworten sind bitte unter Anführung der Geschäftszahl an nis@bka.gv.at zu richten.

Vorarlberger Krankenhaus-
Betriebsges.m.b.H.
Carinagasse 41
6800 Feldkirch

Geschäftszahl: 2020-0.653.319

Bescheid

In dem amtswegig eingeleiteten Verfahren ergeht vom Bundeskanzler gemäß § 4 Abs. 1 Z 6 iVm § 16 Abs. 1 und 4 Z 1 des Netz- und Informationssystemsicherheitsgesetzes (NISG) folgender

Spruch:

Die Vorarlberger Krankenhaus-Betriebsgesellschaft mit beschränkter Haftung mit der Adresse Carinagasse 41, 6800 Feldkirch, und der Firmenbuchnummer 66251d wird gemäß § 16 Abs. 1, 2 und 4 Z 1 NISG als Betreiber wesentlicher Dienste ermittelt. Der von der Vorarlberger Krankenhaus-Betriebsgesellschaft mit beschränkter Haftung betriebene wesentliche Dienst gemäß § 8 Abs. 1 Z 1 lit. a und b der Netz- und

Timeline NIS-G

Zertifizierung der IT-Abteilung nach ISO27001 (Erstausstellung 2019)
(TOMs, ISMS, RM, Richtlinien, usw.)

Auswahl QuaSte

Beauftragung QuaSte

Einreichung Endbericht

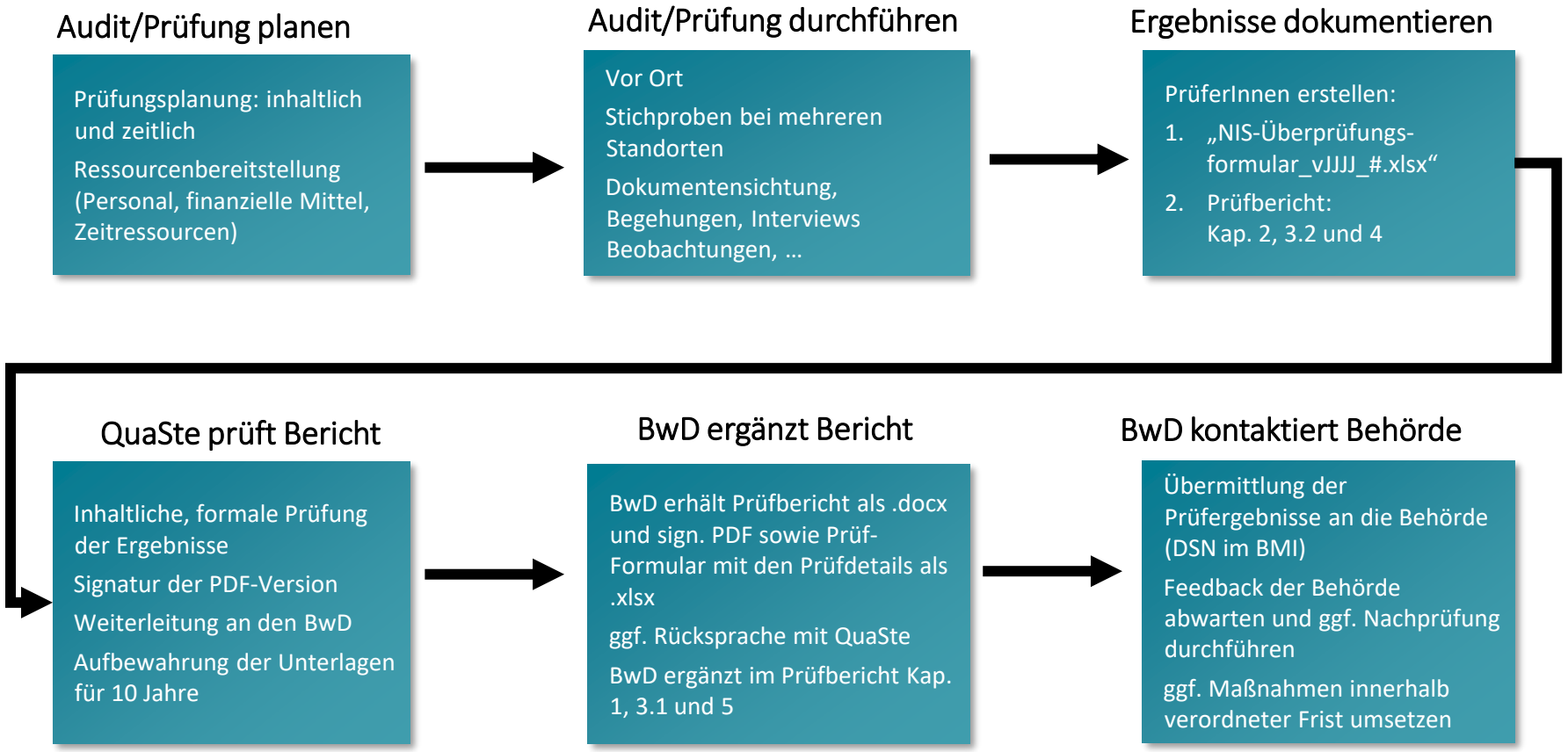
Nov. 2020

Nov. 2021

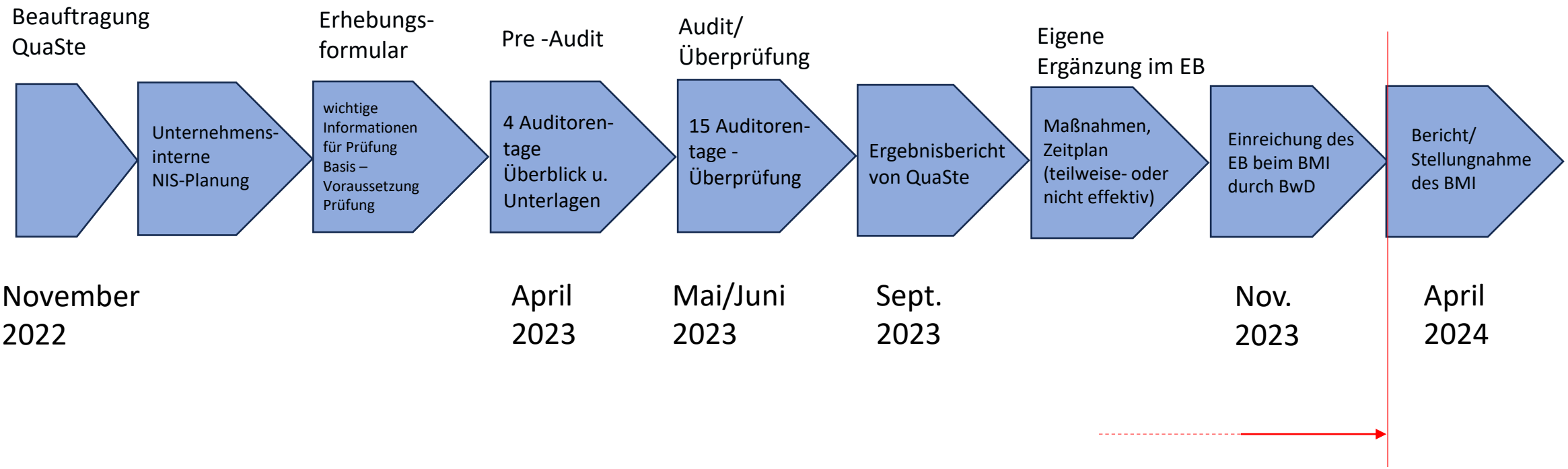
Nov. 2022

Nov. 2023

Ablauf einer NISG-Überprüfung



NIS-G Audit/Überprüfung in der VLKH/KHBG



Beispiel eines Prüfungstages

Datum	Uhrzeit Anfang/ Ende	Norm Kap.-Nr. / Anlage 1 NISV	zu auditierende Prozesse/ notwendige Ressourcen	Teilnehmer/ Abteilung Name/Position	Auditor/Prüfer Name
TAG 6 19.06.23	09:00 – 09:30		Abstimmung Audit-/Prüfungsablauf ggf. offene Fragen		
IT + Informations-dienst: 2,5 Std. Technik + Physik: 1,5 Std.	09:30 – 14:30 *(inkl. 1 Std. Mittags-Pause)*	NIS 4.1 *(ISO A.9.2.3)*	Administrative Zugangsrechte		
		NIS 4.2 *(ISO A.9.4)*	Systeme und Anwendungen zur Systemadministration		
		NIS 6.1 *(ISO A.11.2.4, A.14.1, A.14.2)*	Systemwartung und Betrieb		
ÜBERSICHT + VORBEREITUNG auf TECHNISCHE PRÜFUNGEN					
IT + Informations-dienst: 1,5 Std. Technik + Physik: 0,75 Std.	14:30 – 16:45	NIS 3.1 *(ISO A.12.1.1, A.12.5)*	Systemkonfiguration		
		NIS 3.2 *(ISO A.8.1, A.8.2)*	Vermögenswerte		
		NIS 3.3 *(ISO A.13.1)*	Netzwerksegmentierung		
		NIS 3.4 *(ISO A.12.5., A.12.6)*	Netzwerksicherheit		
		NIS 3.5 *(ISO A.6.1.2, A.8.3, A.10.1, A.11.2.7, A.11.2.9, A.12.2.1, A.12.3.1, A.13.2)*	Kryptographie		

Ausschnitt/Teil Erfassungsformular

3.	**Sicherheitsarchitektur**		
3.1.	Sicherheitsarchitektur	Systemkonfiguration	nicht effektiv
3.2.	Sicherheitsarchitektur	Vermögenswerte	teilweise effektiv
3.3.	Sicherheitsarchitektur	Netzwerksegmentierung	teilweise effektiv
3.4.	Sicherheitsarchitektur	Netzwerksicherheit	teilweise effektiv
3.5.	Sicherheitsarchitektur	Kryptographie	effektiv
4.	**Systemadministrator**		
4.1.	Systemadministrator	Administrative Zugangsrechte	effektiv
4.2.	Systemadministrator	Systeme und Anwendungen zur Systemadministration	nicht effektiv

3.1.: System-/Konfigurationsdokumentation ist vollständig vorhanden	Dokumentation vorhanden	Beschreibung der Abweichung XXX	nicht effektiv	Maßnahmen XXX
3.1.: Konfigurationen sind strukturiert dokumentiert	Vorlagen für Systemdokumentation	Beschreibung der Abweichung XXX	effektiv	Maßnahmen XXX
3.1.: bereits bei der Installation werden Best Practices zur Systemhärtung umgesetzt	Systemhärtung z.B. Standardpasswörter	Beschreibung der Abweichung XXX	effektiv	Maßnahmen XXX
3.2.: Assetslisten mit zumindest jenen Komponenten, die für den BwD relevant sind, sind vorhanden	CMDB vorhanden	Beschreibung der Abweichung XXX	teilweise effektiv	Maßnahmen XXX
3.2.: Absicherung von Systemen/Rechner für Leitwarten udgl. Wird sichergestellt	Überprüfung der Dokumentation	Beschreibung der Abweichung XXX	teilweise effektiv	Maßnahmen XXX
3.2.: Assets (IT-Prozesse, IT-Systeme, IT-Komponeten, Softwareplattformen/-Lizenzen, Applikationen) sind identifiziert, klassifiziert und inventarisiert.	Dokumentation von Netz- und Informationssystem zur Unterstützung von Update- und Patch-Prozess	Beschreibung der Abweichung XXX	effektiv	Maßnahmen XXX
3.3.: die Trennung erfolgt aufgrund des Schutzbedarfs bzw. der Kritikalität des Systems	Netzwerksegmentierung Leitsystem	Beschreibung der Abweichung XXX	nicht effektiv	Maßnahmen XXX

Ausschnitt/Teil eines Ergebnisberichts für BMI

Prüfbericht

eines Betreibers wesentlicher Dienste (Bw
Netz- und Informationssystemsicherheitsge

zur Bewertung der Sicherheitsmaßnahmen gemäß §
Anlage 1 NISV und als Nachweis für einen Betreiber
gemäß § 17 Abs 3 NISG für den Bundesminister für Inr

(gemäß Vorgaben aus NIS Fact Sheet 3/2021 – Version 2).

2.2 Leistungsvereinbarungen mit Dienstleistern und Lieferanten

QuaSte

Effektivitätsbewertung	teilweise effektiv
Gefährdungsbewertung	mittel
Zusammenfassung der Prüfergebnisse	Es wurden für die Fachbereiche IT, Technik und Informationsdienst die Leistungsvereinbarungen mit deren Dienstleistern geprüft. Eine Richtlinie für die Beziehungen zu Dienstleistern und Lieferanten liegt vor, die gelebte Handhabung des Prozesses wurde vorgezeigt und zum Teil von den jeweiligen Mitarbeitern erläutert. Es erfolgte eine stichprobenhafte Überprüfung von Vorgaben und der Dokumentation. Alle Prozesse und Regelungen wurden plausibel begründet und erläutert. Prüfmechanismen für angemessene Sicherheitsmaßnahmen von Dienstleistern sind im Anforderungskatalog zur Anbindung an das IT Netzwerk und dem Dokument Software Bewilligungsantrag festgelegt. Der Fachbereich Technik hat über das Jahr Wartungen durchgeplant, welche planmäßig abgearbeitet werden. Meldungen der Firmen in Bezug auf Medizingeräte erfolgen an den Technischen Sicherheitsbeauftragten. Es sind Vorgaben für Lieferanten und Dienstleister vorhanden, deren MA über einen Zeitraum fix vor Ort sind. (Gemeinsame) Verantwortlichkeiten von Lieferant und BwD sind geklärt und die Einhaltung dieser wird überprüft. Ein Sicherheitsvorfall bei CGM wurde vom Dienstleister und BwD gut abgehandelt. **Prüfhandlungen** gesamt: 13, davon 9 effektiv, 4 teilweise effektiv und 0 nicht effektiv Die Kontaktdaten hinsichtlich Sicherheitsaspekte sind nicht bei allen Dienstleistern (aus den Bereichen IT, Technik, Physik, Informationsdienst) bekannt. Die Erhebung ist aktuell am Laufen, erste

3.2 Vermögenswerte

QuaSte

Effektivitätsbewertung	effektiv
Gefährdungsbewertung	niedrig
g e	Es wurden die Vermögenswerte der vier Fachbereiche geprüft. Die gelebte Handhabung des Prozesses wurde vorgezeigt und zum Teil von den jeweiligen Mitarbeitern erläutert. Die Assets werden von jedem Fachbereich in verschiedenen Systemen geführt. Die Verwaltung der Vermögenswerte (z.B. Umgang mit Updates, Releases) wurde jeweils nachvollziehbar dargestellt. Die gelebten Prozesse und durchgeführten Tätigkeiten wurden plausibel begründet und erläutert. **Prüfhandlungen** gesamt: 12, davon 12 effektiv, 0 teilweise effektiv und 0 nicht effektiv Aufgrund der Feststellungen zu den durchgeführten Prüfkontrollen wurde die Gefährdungslage als „niedrig“ eingestuft.

	Referenz	Maßnahmen	Umsetzungszeitpunkt und Umsetzungsgrad

Bundesministerium
Inneres

bmi.gv.at

BMI - IV/S/2/a (Referat IV/S/2/a)

Ing. Maximilian Schiessl MSc. MSc.
Sachbearbeiter/in

Herrengasse 7, 1010 Wien

E-Mail-Antworten sind bitte unter Anführung der Geschäftszahl an post@nis.gv.at zu richten.

Im Rahmen der elektronischen Zustellung ist das BMI unter der ERsB-ON 9110006619920 adressierbar.

An
Vorarlberger Krankenhaus
Betriebsges.m.b.H.
ergeht per dualer Zustellung

Geschäftszahl: 2023-0.851.271

Stellungnahme zur übermittelten Aufstellung gemäß § 17 Abs. 3 NISG

Sehr geehrte Damen und Herren!

Die ggstdl. Stellungnahme betrifft die Auseinandersetzung mit der am 24.11.2023 übermittelten Aufstellung vorhandener Sicherheitsvorkehrungen der Vorarlberger Krankenhaus Betriebsges.m.b.H. gemäß § 17 Abs. 3 NISG, wobei sämtliche übermittelten Unterlagen miteinbezogen wurden.

Empfehlungen gemäß § 17 Abs. 5 NISG

Zur Herstellung der Anforderungen nach § 17 Abs. 1 NISG ergehen nachfolgende Empfehlungen gemäß § 17 Abs. 5 NISG bezogen auf die jeweilig entsprechend gekennzeichnete Kategorie bzw. Sicherheitsmaßnahme der Anlage 1 zur NISV.

Bei Empfehlungen **mit angeführten Fristen** („30.06.2024, 30.09.2024, und 31.12.2024“) ist die Bestätigung der Umsetzung samt kurzer, nachvollziehbarer Beschreibung der umgesetzten Maßnahmen spätestens bis zum angeführten Zeitpunkt an die Behörde ho. in schriftlicher und konsolidierter Form elektronisch zu übermitteln. Falls dem nicht

Empfehlungen bis 30.06.2024

Ad 2.2 Leistungsvereinbarungen mit Dienstleistern und Lieferanten

- Es wird empfohlen, die SLAs im Bereich Technik und Telekommunikation zu überprüfen.

Siehe hierzu „NIS-Prüfbericht_KHBG-final_v1-0_2023-11_24_1.pdf“:
Kapitel 5 Referenz 2.2 Z 13

Ausschnitt Bericht - QuaSte und BwD (Nov. 2023)

2.2 Leistungsvereinbarungen mit Dienstleistern und Lieferanten

	2.2 Z 13	Überprüfung und ggf. Neureglung der SLA mit wesentlichen Lieferanten im Bereich Technik und Telekommunikation.	30.06.2024

Einige Erfahrungen/Tipps:

- NIS-G als Chance und nicht als Schikane wahrnehmen.
- Früh genug beginnen – es ist sehr viel Arbeit.
  - (von internen Themen bis hin zur Kontrolle von Lieferketten)
- Eigene Ressourcen (Kosten, Personal) vorsehen.
  - (von Projektgruppe - zu einem ständigen Vorhaben)
- Zuständigkeit klar definieren. Es ist nicht nur ein Thema der IT.
  - (die Führung haftet!!!)
  - (Meldeprozesse definieren)
- NIS-Themen Austauschplattformen nutzen – Man ist nicht alleine!
- Wahl der QuaSte gut überlegt.

Danke!