ARBEITSGRUPPE IT

BITS-Labor – Branchenstandard IT-Sicherheit für die Laboratoriumsdiagnostik

Berlin, 3. Mai 2023

ALM Akkreditierte Labore in der Medizin e.V.

Willkommen!

- Workshop
  - mitmachen
  - Fragen stellen
  - Kritik üben
  - Erfahrungen einbringen

ALM Akkreditierte Labore in der Medizin e.V.

Motivation

- Betreiber der kritischen Infrastruktur „Laboratoriumsdiagnostik“ bei der Umsetzung der Anforderung aus §8a BSIG zu unterstützen
- Arbeitsaufwand reduzieren
- Handlungsempfehlungen (Best Practice) zu geben
- Erfahrung zu teilen
- Rahmen für den Nachweis zu beschreiben
- Prüfung erleichtern

Warum (z. Zt.) kein B3S

- Bereits im Jahr 2018 hatte der ALM e.V. die erste Version eines Branchenspezifischen Sicherheitsstandards (B3S Labor) beim Bundesamt für Sicherheit in der Informationstechnik (BSI) eingereicht und in einer finalen Version 1.01 konsentiert. Die Feststellung der Eignung als Branchenspezifischer Sicherheitsstandard (B3S Labor) erfolgte am 21.01.2019 durch das BSI.
- Das Prüfverfahren für den Entwurf des B3S Labor 2.0, der im Juni 2022 beim BSI eingereicht wurde, konnte nicht im notwendigen zeitlichen Rahmen abgeschlossen werden. Auf Grund der dringenden Notwendigkeit einer geeigneten Prüfungsgrundlage hat sich der ALM e.V. dazu entschieden, dieses Dokument als Branchenstandard IT-Sicherheit für die Laboratoriumsdiagnostik (BITS) ohne weitere Verzögerung in geeigneter Weise der Fachöffentlichkeit zugänglich zu machen.

- **Wir wollen den B3S aber weiterentwickeln!**

Was sagt das Gesetz?

- Scope
  Betreiber [sind verpflichtet], **angemessene** organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer **informationstechnischen** Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen **maßgeblich** sind.
- Grenzen
  Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche **Aufwand** nicht außer **Verhältnis** zu den Folgen eines **Ausfalls** oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.
- Maß
  Dabei soll der Stand der Technik eingehalten werden.
  - in der Fachpraxis erprobt und bewährt
  - von der Mehrheit der Fachleute anerkannte Regeln und Standards

Was ist nicht gefordert

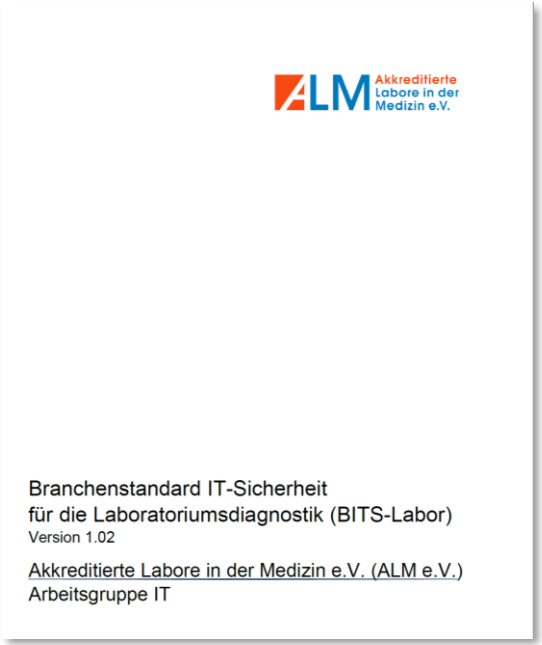
- Zertifizierung nach Grundschutz, ISO 27001 etc.
  - Die Betreiber Kritischer Infrastrukturen haben [..] die Erfüllung der Anforderungen [..] auf **geeignete Weise** nachzuweisen. (KANN Sicherheitsaudits, Prüfungen, Zertifizierungen)
- weitergehende regulatorische oder sonstige Vorgaben
  - DSGVO, BCMS
- Anforderungen, Maßnahmen aus anderen (KRITIS) Bereichen
  - Labor ist keine Bank (kein MaRisk, kein BAIT etc.)
- keine Prüfung nach Normenvorgaben (Audit, Ja/Nein, erfüllt/nicht erfüllt)
  - Angemessenheit, Reifegrad, risikoabhängig

Aber: Stand der Technik im Laborumfeld (Fachliteratur, B3S)

BITS & Arbeitshilfe

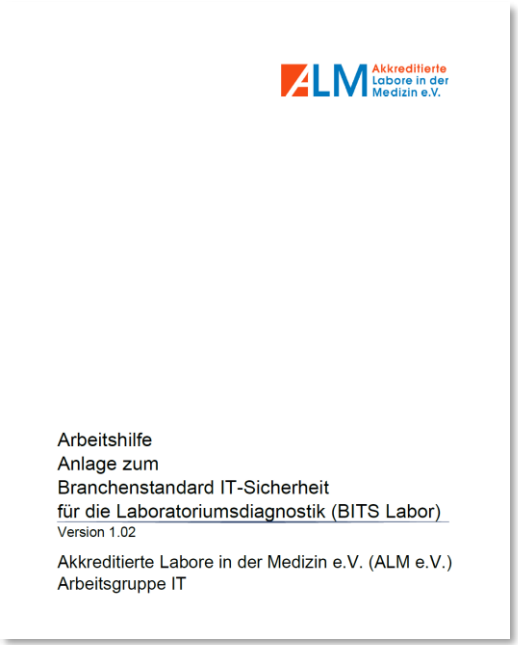
- Sicherheitsstandard für die Laboratoriumsdiagnostik aus Fachkreisen
- Herausgegeben vom Branchenverband ALM
- Strukturgleich einem B3S s. a. Orientierungshilfe .....
- baut auf Grundschutz auf
- Definiert Scope der kDl
- bietet Risikoanalyse für kDl
- zeigt Maßnahmen zur Absicherung der kDl nach Stand der Technik auf u. a. Anforderungsliste
- Hilfestellung für Betreiber zur Erhöhung der IT-Sicherheit BITS
- Hilfestellung für Prüfer bei der Erstellung des Prüfplans Arbeitshilfe

BITS & Arbeitshilfe



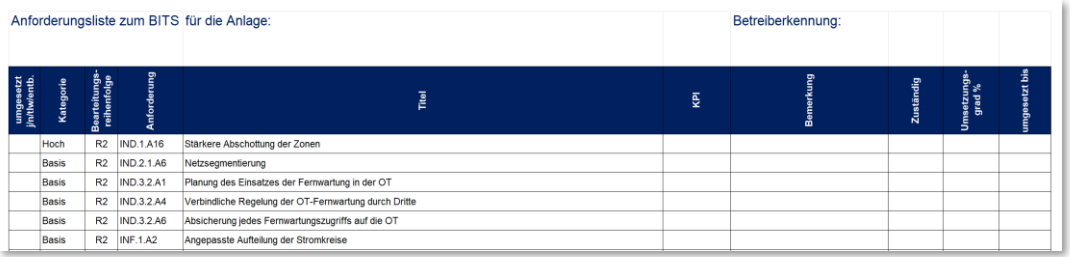
Branchenstandard IT-Sicherheit
für die Laboratoriumsdiagnostik (BITS-Labor)
Version 1.02

Akkreditierte Labore in der Medizin e.V. (ALM e.V.)
Arbeitsgruppe IT



Arbeitshilfe
Anlage zum
Branchenstandard IT-Sicherheit
für die Laboratoriumsdiagnostik (BITS Labor)
Version 1.02

Akkreditierte Labore in der Medizin e.V. (ALM e.V.)
Arbeitsgruppe IT



Anforderungsliste zum BITS für die Anlage: Betreiberkennung:

umgesetzt ja/n/wenn.	Kategorie	Bearbeitungs-reihenfolge	Anforderung	Titel	KPI	Bemerkung	Zuständig	Umsetzungs-grad %	umgesetzt bis
	Hoch	R2	IND.1.A16	Stärkere Abschottung der Zonen					
	Basis	R2	IND.2.1.A6	Netzsegmentierung					
	Basis	R2	IND.3.2.A1	Planung des Einsatzes der Fernwartung in der OT					
	Basis	R2	IND.3.2.A4	Verbindliche Regelung der OT-Fernwartung durch Dritte					
	Basis	R2	IND.3.2.A6	Absicherung jedes Fernwartungszugriffs auf die OT					
	Basis	R2	INF.1.A2	Angepasste Aufteilung der Stromkreise					

BITS

Inhaltsverzeichnis

ALM Akkreditierte Labore in der Medizin e.V.

Arbeitshilfe

Tabellen

Grafiken

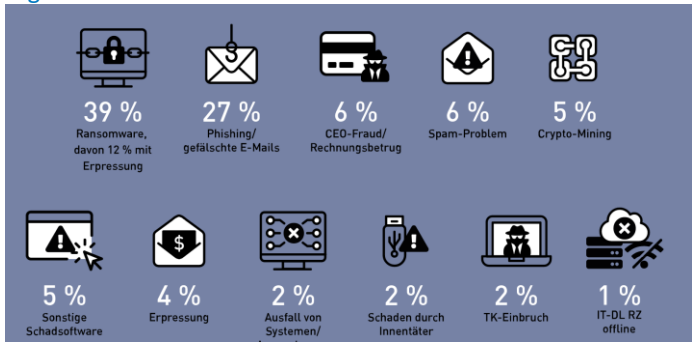
Prüfung

- an den Gegebenheiten ausrichten
  - Informationsverbund Ja/Nein
  - Beitrag zur Erbringung zur kDl (z.B. Durchsatz)
  - Kritikalität nach Einschätzung des Betreibers (z.B. Kommunikationswege)
  - nicht technische „work-arounds“ sind auch ein Control
- Nicht jede Control des BITS ist auf jedes Labor anwendbar
  - Infrastruktur gibt Control nicht her z.B. INF.2.A8 Einsatz einer Brandmeldeanlage
  - Reifegrad des Labors ermöglicht keine Umsetzung z.B. ISMS ist erst im ersten Zyklus
  - Control hat mehr „informativen“ Charakter DER.2.1.A6 Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen

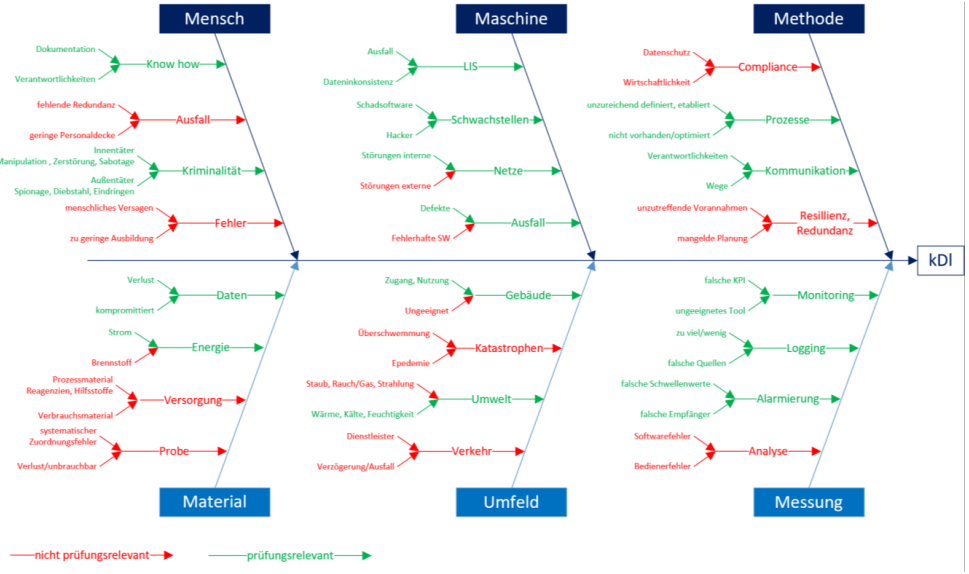
→ angepasste Anforderungsliste

Risiko

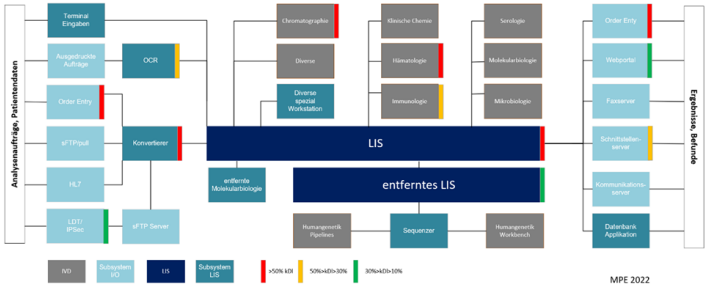
allgemeines Risiko



prozesspezifisches Risiko (kDl)



anlagenspezifisches Risiko



Phasen

	Prüfung	Fragen	Vorgehen	
0	**Vorbereitung**	Focus der Prüfung? Risiko bekannt?	Prüfplan	Scope, Assets, Prozesse, Modellierung
1	**Grundlagen**	KRITIS-Ansatz nachvollziehbar und plausibel?	Review Dokumente Interview Verantwortliche	Informationstechnische Systeme (Assets) und Organisation „matchen“ der kDl
2	**Angemessenheit**	Maßnahmen angemessen geplant und umgesetzt?	Interview Experten Review Maßnahmen + IT	Wird dem Risiko angemessen begegnet
3	**Wirksamkeit**	Maßnahmen wirklich im Einsatz und wirksam?	Review Nachweise Stichproben IT	
∑	**Berichterstattung**	Nachweisdokumente		Reifegrad, Bewertung der Maßnahmen

aus https://www.openkritis.de/pruefung/bsig-nachweispruefung-8a-3-kritis.html

BiTS zur Unterstützung der Prüfung

- scope → S. 12 Grafik 4: kDL Lab Prozess
  → S. 13 1.1.3 Anwendungsbereich (Abgrenzung)
  → S. 37 4.3.2 Modellierung eines übergreifenden Informationsverbundes
  Netzwerkplan → S. 31 Grafik 7: Typisches Labornetzwerk nach Grundschutz (Beispiel)
- Risiko → S. 18 Tabelle 5: Direkt relevante Gefährdungen
  → Arbeitshilfe S. 7
    - 1.3.2 Nach Risikoeinflussfaktoren
    - Grafik 4: Datenfluss und Kritikalität (Beispiel)
- Schutzbedarf → S. 16 1.4.3 Systemspezifische Schutzziele
- ISMS → S. 25 Tabelle 9: Sicherheitsrichtlinien
- SzA → S. 34 4.1.9 Überprüfung im laufenden Betrieb ….
- Controls → Anforderungsliste
- für Prüfer → Arbeitshilfe zum BITS

Systeme zur Angriffserkennung

- organisatorische und technische Vorkehrungen [..] ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung
  - Controls: 4.1.9 Überprüfung im laufenden Betrieb / Vorfalls-/Angriffserkennung & Bearbeitung
    - Protokollierung
    - Virenscanner
    - 2. Gen. Firewall
    - Organisation
  - Feststellen des Reifegrads nach dem „Umsetzungsgradmodells“

Reifegrad

Reifegrad	Bedingung
0	keine Maßnahmen umgesetzt
1	Maßnahmen geplant nicht alle MUSS umgesetzt
2	Maßnahmen in Umsetzung nicht alle MUSS umgesetzt
3	alle MUSS umgesetzt KVP in Planung/etabliert
4	alle MUSS & SOLLTE umgesetzt KVP etabliert
5	alle MUSS, SOLLTE &KANN umgesetzt KVP (kontinuierlicher Verbesserungsprozess) etabliert zusätzliche Maßnahmen nach Analyse

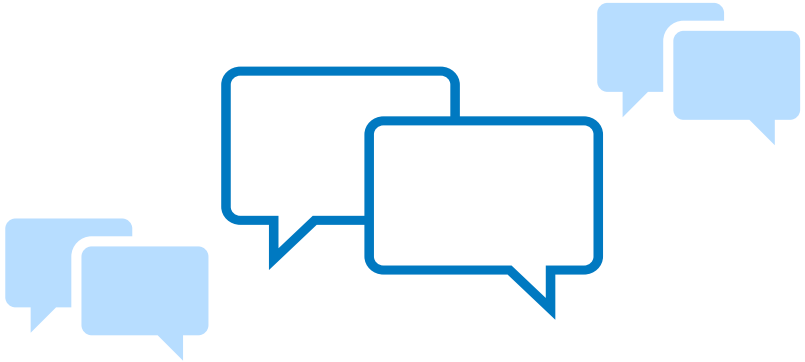
- Bei der Wahl geeigneter Maßnahmen zur Erfüllung der Anforderungen ist der Betreiber frei.

www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf

Beste aller Welten

- Prüfer und Betreiber arbeiten Hand-in-Hand
- Risikobasierter Ansatz,
- Mehrwert für den Betreiber zu generieren: Erhöhung der Sicherheit und Resilienz seines Geschäftsprozesses
- Weiterentwicklung anzuregen
- Blinde Flecken zu erhellen, weitere Wege aufzuzeigen
- IST-Zustand fair und mit technischem Sachverstand darzustellen
- ganzheitliche Betrachtung des zu prüfenden Informationsverbundes mit Focus auf die Kernkomponenten der kDl

- **Ziel: kDl abzusichern**



Fragerunde

Akkreditierte Labore in der Medizin – ALM e.V.
Invalidenstraße 113 (HELIX HUB), 10115 Berlin

kontakt@alm-ev.de
@ALMevTeam
www.alm-ev.de

Lobbyregister: R001160