interim management & industrial support

imis consulting

INTERIM MANAGEMENT & INDUSTRIAL SUPPORT

HINWEIS

Gender-Formulierung

Aus Gründen der besseren Lesbarkeit wird in dieser Präsentation vorrangig die männliche Form verwendet. Bei allen personenbezogenen Bezeichnungen meint die gewählte Formulierung stets alle Geschlechter und Geschlechtsidentitäten.

Die verkürzte Sprachform hat rein redaktionelle Gründe und ist wertfrei.

Haftungsausschluss

Die in diesem Dokument dargestellten Informationen spiegeln die aktuelle Meinung der imis consulting zum Zeitpunkt der Veröffentlichung zu den betreffenden Themen wider. Dieses Dokument dient ausschließlich zu Informationszwecken.

Es ist weder rechtlich bindend noch privilegiert es irgendjemanden. Es spiegelt nicht notwendigerweise die Meinung genannter Organisationen sowie der Aufsichtsbehörden wider.

Copyright

* Im Zusammenhang mit dieser Mitteilung bezeichnete „intern“ die Organisation des Kunden. „Extern“ bezeichnet jeden anderen Bereich, der nicht strikt mit der Organisation des Kunden zusammenhängt. Z.B. gelten produkt- oder servicebezogene Veranstaltungen als externe Veranstaltungen.

DATENINTEGRITÄT IM AKKREDITIERTEN LABOR

- Definitionen
- Risiken und Gefährdungen
- Grundlagen und Herausforderungen
- Data Governance
- Kultur für Datenintegrität
- Rollenkonzepte
- Kritische Daten
- ALCOA (+/++)
- Data Life Cycle
- Risikomanagement
- Sicherheitsmaßnahmen
- CSV
- Fazit

Foto von Buffik auf Pixabay

DEFINITIONEN „DATENINTEGRITÄT“

Wikipedia:

The maintenance of, and the assurance of, data accuracy and consistency over its entire life-cycle. It is a critical aspect to the design, implementation, and usage of any system that stores, processes, or retrieves data.

WHO:

The degree to which data are complete, consistent, accurate, trustworthy and reliable and that these characteristics of the data are maintained throughout the data life cycle. The data should be collected and maintained in a secure manner (ALCOA) [1]

MHRA 2018:

The extent to which all data are complete, consistent, and accurate throughout the data life-cycle. [2]

FDA:

The completeness, consistency, and accuracy of data. Complete, consistent, and accurate data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate (ALCOA). [3]

PIC/S:

the degree to which data are complete, consistent, accurate, trustworthy, and reliable, and that these characteristics of the data are maintained throughout the data life cycle. [4] (see MHRA)

RISIKEN FÜR DATENINTEGRITÄT

- ! Fehlerhafte Datenerfassung
- ! Fehlende Rückverfolgbarkeit
- ! Datenverlust / -manipulation
- ! Unzureichende CS-Validation
- ! Datenverwaltung / Zugriffsrechte
- ! Verletzung regulatorischer Anforderungen
- ! Prozessabweichungen / Fehlverhalten
- ! Kommunikationsfehler

Foto von Peggy und Marco Lachmann-Anke auf Pixabay

WANN IST DIE DATENINTEGRITÄT GEFÄHRDET?

NACHVOLLZIEHBARKEIT

Wer hat wo, was , wann, wie und warum gemacht hat?

DOKUMENTATION

Festgelegten Prozess zur Dokumentation?

SELEKTION

Anwendung von Filtern bei Berichten, Reviews oder bei der Analyse

MANIPULATION

Daten werden verändert, ergänzt oder „fallen unter den Tisch“

BEWERTUNG

Abstimmung/Bewertung vor der Erfassung

LÖSCHUNG/VERNICHTUNG

Festgelegter Prozess zur Handhabung der Daten? Bewusste Vernichtung?

GRUNDLAGEN DER DATENINTEGRITÄT IM AKKREDITIERTEN LABOR

Kombination verschiedener Konzepte als Grundlage für die Anforderungen an die Datenintegrität z.B. in der DIN EN ISO/IEC 17025

Etablierung von Prozessen zur Kontrolle und Sicherstellung der Datenqualität	**QM-SYSTEME**
Schutz von Daten vor unbefugtem Zugriff, Änderungen, Verlust	**IT-SECURITY**
Detaillierte Richtlinien zur Erfassung, Speicherung und Berichterstattung	**REGULATORIEN**
Herkunft und Bearbeitung von Daten klar dokumentieren.	**ALCOA / ALCOA+**
Klare Vorgaben an Dokumentationen / Aufzeichnungen	**GDP bzw. GDocP**

SPEZIELLE ANFORDERUNGEN IM AKKREDITIERTEN LABOR

ISO 17025, Kap. 7.11.2: [5]

Die Informationsmanagementsysteme des Laboratoriums [, ...], müssen vor ihrer Einführung auf ihre Funktionsfähigkeit hin bewertet werden. Das schließt das ordnungsgemäße Funktionieren von Schnittstellen innerhalb der Informationsmanagementsysteme des Laboratoriums ein. Bei Änderungen, einschließlich Änderungen an der Softwarekonfiguration oder –Modifikation an kommerzieller Standardsoftware des Laboratoriums, müssen diese vor der Umsetzung validiert, freigegeben und dokumentiert werden.

ISO 17025, Kap. 7.11.3:

Das Informationsmanagementsystem des Laboratoriums muss:

a) vor unbefugtem Zugriff geschützt sein;

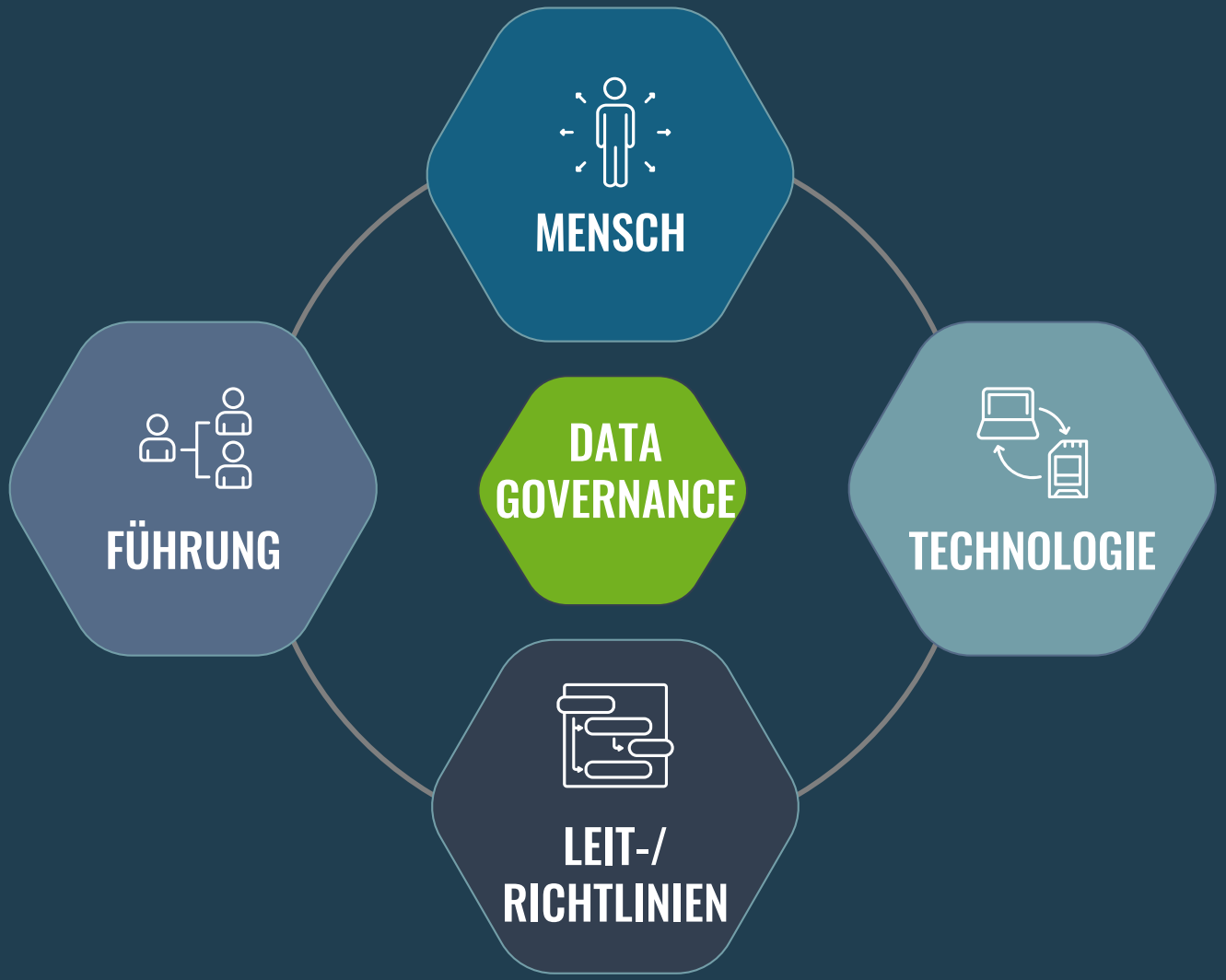
b) gegen Manipulation und Verlust gesichert sein;

c) in einer Umgebung betrieben werden, welche den Spezifikationen des Anbieters oder des Laboratoriums entspricht, oder im Fall von nicht rechnergestützten Systemen Bedingungen vorhält, die die Genauigkeit bei manueller Aufzeichnung und Übertragung sicherstellen;

d) in einer Weise aufrechterhalten werden, die die Unversehrtheit der Daten und Informationen sicherstellt;

e) die Aufzeichnung von Systemausfällen sowie die angemessenen Sofort- und Korrekturmaßnahmen mit einschließen.

HERAUSFORDERUNGEN FÜR DIE DATENINTEGRITÄT



ASPEKTE DER DATA GOVERNANCE

- Genau
- Vollständig
- Konsistent
- Original

- Unbefugter Zugriff
- Manipulation
- Datenverlust

- Data Management
- Data Inventory Management
- Data Incident Management
- Datenarchitektur
- Dateninfrastruktur

- Wer?
- Wann?
- Wie?

- Gesetze
- Regularien

KULTUR DER DATENINTEGRITÄT

- Grundsätze, Werte und Visionen vorleben
- Mitarbeiter in Führungsrollen coachen
- Ressourcen

- Formelle / informelle Qualitätsdiskussionen
- Bedeutung von DI im Unternehmen
- Kontinuierliches Lernen und Verbessern

- Engagement der Führung
- Offener und ehrlicher Dialog
- Mitarbeiter coachen / betreuen
- Fortschritt der Verhaltensänderung
- Kommunikation

- Ziele identifizieren
- Verhaltensweisen beeinflussen
- Bewusstsein fördern
- Problemidentifikation

- Angleichung von Qualitätszielen
- Überwachung zur kontinuierlichen Verbesserung
- Beteiligung von Mitarbeitern u. Management
- Audits und Reviews

- «Lernende» Organisation
- Schulung der Mitarbeiter
- Kontinuierliche Verbesserungen
- Echte Ursachenanalyse

«KULTUR DER EXZELLENZ»[7]

ROLLENKONZEPTE UND ZUSTÄNDIGKEITEN (1/2)

Senior Management	Gesamtverantwortung für die Einhaltung aller regulatorischen Anforderungen und der Anforderungen an die Datenintegrität; Förderung einer Unternehmenskultur, die die Bedeutung der DI betont; Bereitstellen der notwendigen Ressourcen zur Sicherstellung, dass das DI-Konzept umgesetzt werden kann; Festlegung von strategischen Zielen u. Richtlinien zur DI; Überwachung u. Review zur DI-Performance
Datenintegritäts-beauftragter	Entwicklung und Implementierung von Datenintegritätsprogrammen und -richtlinien; Durchführung von Risikoanalysen u. Identifikation von Schwachstellen zur DI; Schulung u. Sensibilisierung der MA; Überwachung u. Bewertung der Wirksamkeit der Maßnahmen zur Sicherstellung der DI; Bericht an Senior Management
Prozess-eigner	Leitendes Mitglied der Abteilung, die das System verwendet; Sicherstellen, dass Prozess die Anforderungen an DI erfüllt; Implementieren u. Überwachen von Kontrollmechanismen innerhalb der Prozesse; Kontrolle des Zugangs zum System zusammen mit Systemeigner; verantwortlich für CS u. Betrieb im Einklang mit SOPs u. „Intended Use“; Schulung MA; SOPs, Change Management, CAPAs, Audits u. Review
System-eigner	Verantwortung für die DI des zugewiesenen Systems; Sicherstellung des DI-konformen Betriebs des Systems; Zusammenarbeit mit System-Entwickler u. –Support zur Gewährleistung der DI bei allen Systemänderungen; Dokumentation u. Überwachung von Systemänderungen u. derer Auswirkungen auf die DI
System-support	Technischer Support u. Wartung der Systeme zur Sicherstellung der DI; Durchführungen von Validierungen u. Verifizierungen, um sicherzustellen, dass Systeme korrekt u. zuverlässig funktionieren; Überwachung u. Behebung technischer Probleme, die die DI beeinträchtigen könnten; Zusammenarbeit mit Systemeigner zur Implementierung von DI-Verbesserungen
Datenbank-administrator	Verwaltung u. Wartung der Datenbanken zur Sicherstellung der DI; Implementierung von Backup- u. Wiederherstellungsverfahren zum Schutz der DI; Überwachung von DB-Aktivitäten zur Erkennung interner oder externer Korruption; Sicherstellung der Datenkonsistenz, -vollständigkeit und –genauigkeit durch regelmäßige Überprüfungen

ROLLENKONZEPTE UND ZUSTÄNDIGKEITEN (2/2)

Daten-verwalter	Verwaltung u. Pflege der Datenbestände gem. DI-Richtlinien; Sicherstellung, dass Daten korrekt erfasst, gespeichert und verarbeitet werden; Durchführung von Datenqualitätsprüfungen und –validierungen; Dokumentation von Datenmanagementprozessen u. Sicherstellung der DI über gesamten Datenlebenszyklus hinweg
Daten-eigentümer	Verantwortung für die Richtigkeit, Vollständigkeit u. Integrität der ihnen zugewiesenen Daten; Festlegung von Zugriffs- u. Berechtigungsrichtlinien für die daten; Zusammenarbeit mit Datenverwalter u. anderen zur Sicherstellung der DI; Überwachung der Datenqualität u. Durchführung regelmäßiger Datenreviews
Qualität	Unabhängige Überwachung u. Prüfung zur Integrität der Daten während des gesamten Daten-Lebenszyklus; Durchführung von Audits u. Inspektionen zur Überprüfung der DI; Entwicklung von QM-Systemen, die DI-Anforderungen integrieren; Schulung der MA
Fach-experte	Bereitstellung fachlicher Expertise (SME) zur Sicherstellung der DI in spezifischen Bereichen; Unterstützung bei Entwicklung u. Implementierung von DI-Maßnahmen; Durchführung von Reviews u. Bewertungen der DI im spezifischen Fachbereich; Beratung der Prozessverantwortlichen u. des Senior Managements in Fragen der DI
End-user	Einhaltung von DI-Richtlinien u.-prozesse bei der Datenerfassung u. –verarbeitung; Meldung von DI-Problemen oder –verdachtsfällen an den zuständigen Support oder DI-Beauftragten; Teilnahme an Schulungen u. Weiterbildungen zur DI; Sorgfältiger Umgang mit Daten u. Bewusstsein für die Bedeutung der DI im täglichen Arbeitsablauf
System-entwickler	Umsetzung der Nutzeranforderung u. Entwicklung des Systems entsprechend der festgelegten Verfahren unter Beachtung von DI-Anforderungen; Durchführung von Validierungen u. Tests zur Sicherstellung der DI; Zusammenarbeit mit Systemeigner u. –support zur Sicherstellung, dass Systemänderungen die DI nicht beeinträchtigen; Dokumentation von Systementwicklungen u. -änderungen

DAS ALCOA (+/++)-PRINZIP (1/2)

A	ZUWEISBAR (Attributable)	• Alle Daten müssen einer bestimmten Quelle / Person / System zugeordnet werden können, die/das die Daten generiert hat oder eine Aktivität ausführt, bei der Daten erstellt oder geändert werden (Verknüpfung / Rückführbarkeit zur Quelle der Daten)
L	LESBAR (Legible)	• Daten müssen dauerhaft sowie klar und deutlich lesbar sein (Speicherung dauerhaft auf geeigneten Medien) • Zugänglich während des gesamten Lebenszyklus • Originaldaten und spätere Änderungen werden nicht verschleiert
C	ZEITGENAU (Contemporaneous)	• Daten sollen zum Zeitpunkt der Datenerhebung aufgezeichnet werden, nicht im nachträglich • Aufzeichnung oder Beobachtung zum Zeitpunkt der Durchführung der Aktivität
O	ORIGINAL (Original)	• Es muss sich um Originaldaten handeln oder um eine zugelassene Kopie (Kopie muss erkennbar sein) • Originaldaten sind die erste Aufzeichnung von Daten oder eine „echte Kopie“, die Inhalt oder Bedeutung bewahrt
A	GENAU (Accurate)	• Alle Daten müssen korrekt, präzise und frei von Fehlern sein • Keine Bearbeitung ohne dokumentierte Änderungen • Die Daten müssen der Wahrheit oder Norm entsprechen

[...]

DAS ALCOA (+/++)-PRINZIP (2/2)

[...]

VOLLSTÄNDIG
(**C**omplete)

- Alle Daten inkl. relevanter Metadaten, einschl. aller durchgeführter Wiederholungen u. neuer Analysen, müssen vollständig und ohne Auslassungen vorliegen

+

KONSISTENT
(**C**onsistent)

- Daten sollen konsistent u. logisch zusammenhängend sein, die Anwendung von Datums- u. Zeitstempeln in erwarteter Reihenfolge
- Anwendung einer guten Dokumentationspraxis (GDocP) in jedem Prozess

DAUERHAFT
(**E**nduring)

- Aufbewahrung von Daten in einer Weise, die ihre langfristige Verfügbarkeit und Zugänglichkeit sicherstellt
- Aufzeichnung in dauerhafter, aufbewahrungsfähiger Form für die Dauer der Aufbewahrungsfrist

VERFÜGBAR
(**A**vailable)

- Verfügbar während der gesamten Aufbewahrungsdauer, wenn sie benötigt werden und zugänglich für Überprüfungen, Audits und Inspektionen

10
++

RÜCKVER-FOLGBARKEIT
(**Traceable**)

- Daten sollen während des gesamten Lebenszyklus nachvollziehbar sein
- Alle Änderungen an Daten, am Kontext und an Metadaten müssen nachvollziehbar sein (Audit Trail)

KRITISCHE DATEN

A ROHDATEN

B KALIBRIERDATEN

C QUALITÄTSKONTROLLDATEN

D PROBEN- U. ANALYSEDATEN

E DATEN ZUR RÜCKVERFOLGBARKEIT

UMGANG MIT KRITISCHE DATEN

01

DOKUMENTATION & SPEICHERUNG

02

VERIFIZIERUNG & VALIDIERUNG

03

RÜCKVERFOLG-BARKEIT

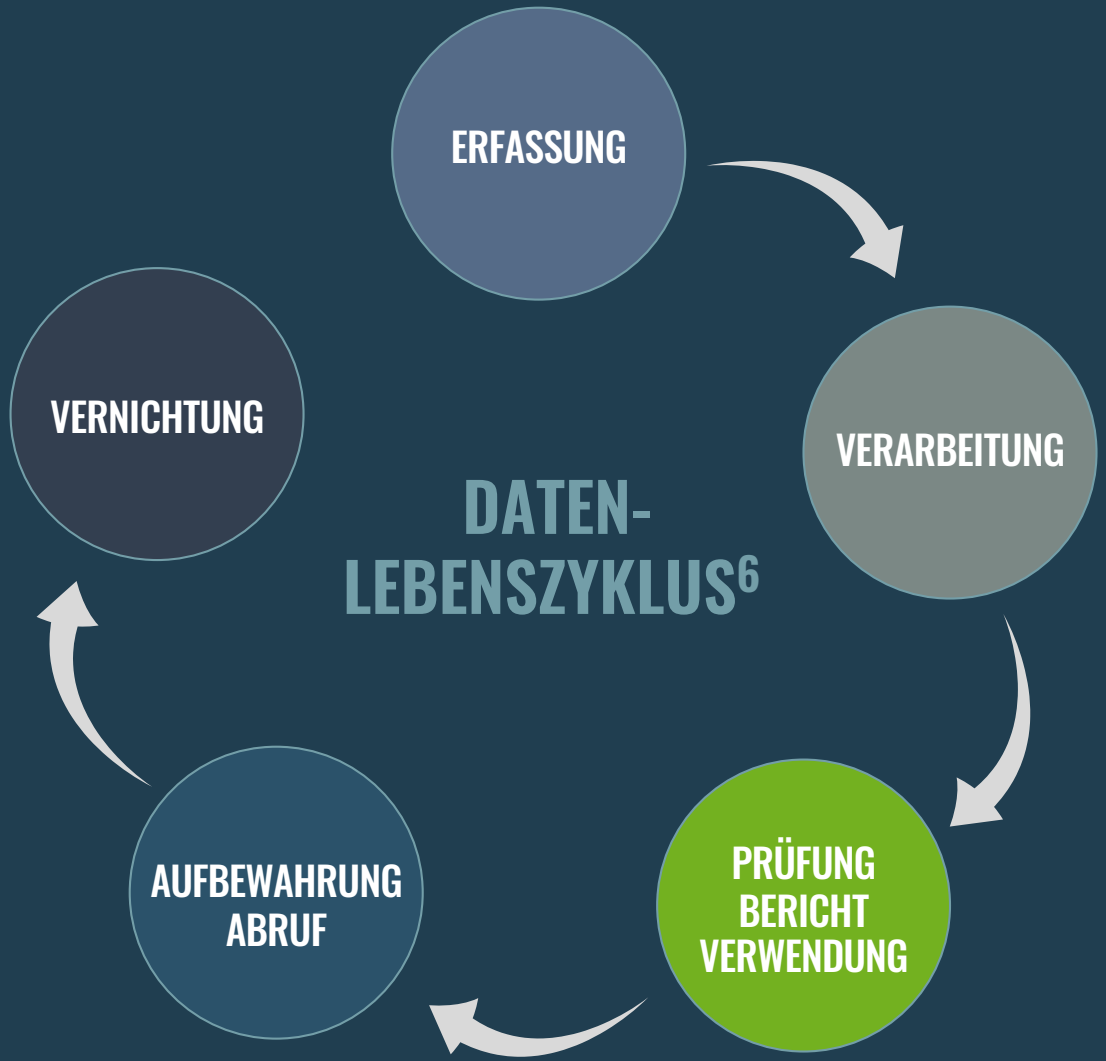
04

ZUGRIFFS-KONTROLLEN

05

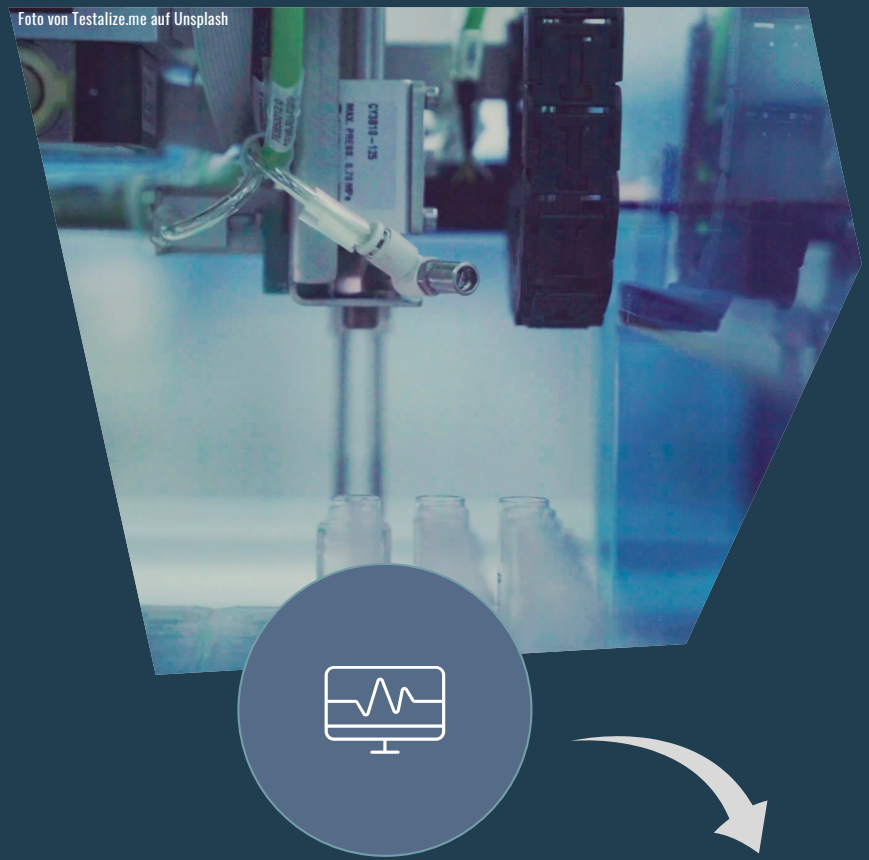
ARCHIVIERUNG & AUFBEWAHRUNG

LEBENSZYKLUS VON DATEN



- Gewährleistung der Datenintegrität während des gesamten Lebenszyklus der Daten
- Einhaltung der ALCOA(+/++)-Prinzipien in jedem Stadium des Zyklus

LEBENSZYKLUS VON DATEN - ERFASSUNG



DATENERFASSUNG

- Korrekt, genau und vollständig
- Inhalt und Bedeutung
- Wartung u. Kalibrierung des Datenerfassungssystems
- Automatische Datenerfassung (wo möglich)
- Direkte Speicherung der Daten („contemporaneous“)
- Zugangskontrollen für Rechte zur Datenänderung
- TOMs zur Gewährleistung der Manipulationssicherheit
- ...

LEBENSZYKLUS VON DATEN - VERARBEITUNG

- Die Erfassung und Speicherung in einem für die Weiterverarbeitung geeigneten Format
- Anwendung definierter und geprüfter Prozesse (z.B. validierte Spreadsheets)
- Sicherung aller Originaldaten
- Rechteverwaltung für Zugriff auf gesicherte Daten
- Änderungsnachverfolgung bei benutzerdefinierten Änderungen
- Nachvollziehbarkeit von Änderungen (Audit Trail / Change Management)
- ...

Foto von Tima Miroshnichenko auf Pexels

DATENVERARBEITUNG

LEBENSZYKLUS VON DATEN – PRÜFUNG (1)

Foto von Thirdman auf Pexels

- Überprüfung von Originaldaten (oder „echte Kopie“)
- Prüfung von Metadaten und Audit Trail
- Dokumentierter Freigabeprozess für Daten
- Einhaltung der TOMs
- Wie wird mit atypischen, fehlerhaften oder ungültigen Ergebnissen verfahren?

DATENPRÜFUNG

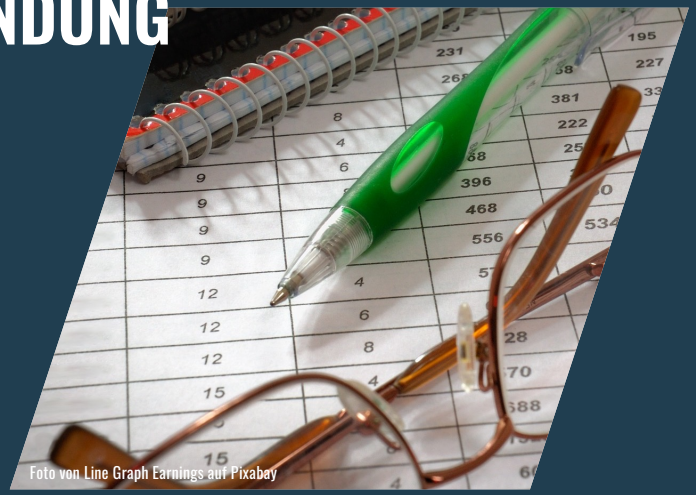
LEBENSZYKLUS VON DATEN – PRÜFUNG (2)

- Dokumentation aller Änderungen und Aktionen an Daten
- Personenbezogen und sicher
- Zeitstempel
- Rekonstruktion von Erzeugung, Modifikation und Löschung
- Audit Trail immer aktiviert
- Rechtekonzept für Personen, die Review durchführen
- Möglichkeit eines (selektierten) Reports
- Wie wird mit Auffälligkeiten verfahren? - Gefahr des Verlusts der Datenintegrität!
- ...

AUDIT TRAIL

Foto von Kelly Sikkema auf Unsplash

LEBENSZYKLUS VON DATEN – BERICHT / VERWENDUNG



DATEN-BERICHT

- Bericht basierend auf erfasste, verarbeitete und gespeicherte Daten
- Genau, vollständig, nachvollziehbar, konsistent, unverändert… (→ ALCOA+/++)
- Unterstützung von Entscheidungen (z.B. Freigabe), Compliance und regulatorischen Anforderungen
- Validierter Prozess zur Berichterstellung
- Kontrollierter Zugang zu Berichtsprozessen

LEBENSZYKLUS VON DATEN – SPEICHERUNG

- Sicherer Speicherort für festgelegten Aufbewahrungszeitraum (Prozessbeschreibung / SOP)
- Verfügbarkeit über definierten u. geprüften Prozess
- Vorgaben für Datenschutz?
- Zugangsbeschränkung / Serverarchitektur
- Schutz vor Elementarschäden
- Speicherung zum Zeitpunkt der Tätigkeit?
- Datenübernahme in andere Systeme
- Adresssynchronisation bei Speicherung auf mehreren Servern
- Disaster Recovery (validiertes Backup & Wiederherstellung)
- Eignung der Speichermedien
- Verschlüsselungstechniken

DATEN-SPEICHERUNG

Foto von Zaid Mohammed auf Pexels

LEBENSZYKLUS VON DATEN – ARCHIVIERUNG

DATEN-ARCHIVIERUNG

Foto von Pexels auf Pixabay

- Langfristig / dauerhaft
- Über den gesamten Aufbewahrungszeitraum
- Daten u. zugehörige Metadaten zur Gewährleistung der Nachvollziehbarkeit
- Lebenserwartung der Speichermedien?
- Medienwechsel / Migration?
- Medienverwaltung (Zugangskontrolle)
- Anzahl Kopien?
- Was passiert bei einem System-Upgrade? / Technologiewandel?
- Gibt es ein SLA bei der Auslagerung der Daten?
- Regelmäßige Prüfung der Verfügbarkeit

LEBENSZYKLUS VON DATEN – VERNICHTUNG

- Welche Anforderungen gibt es für die Aufbewahrung?
- Wer autorisiert die Daten-Löschung?
- Die Löschung der Daten sollte von allen Systemen und physischen Standorten erfolgen
- Maßnahmen zur Vermeidung versehentlichen Löschens
- Dokumentation der Daten-Vernichtung
- Zugangsbeschränkung / Rechte

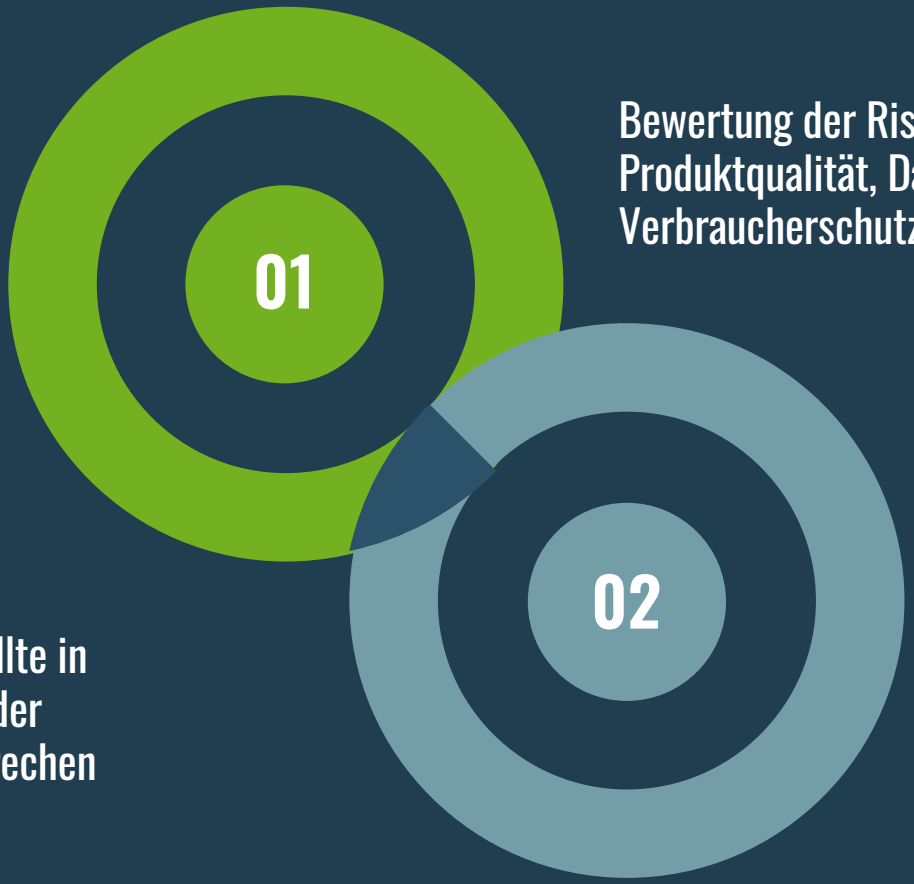
DATEN-VERNICHTUNG

Foto von Wilfried Pohnke auf Pixabay

RISIKOMANAGEMENT - GRUNDSÄTZE

GEFÄHRDUNGS-BEURTEILUNG

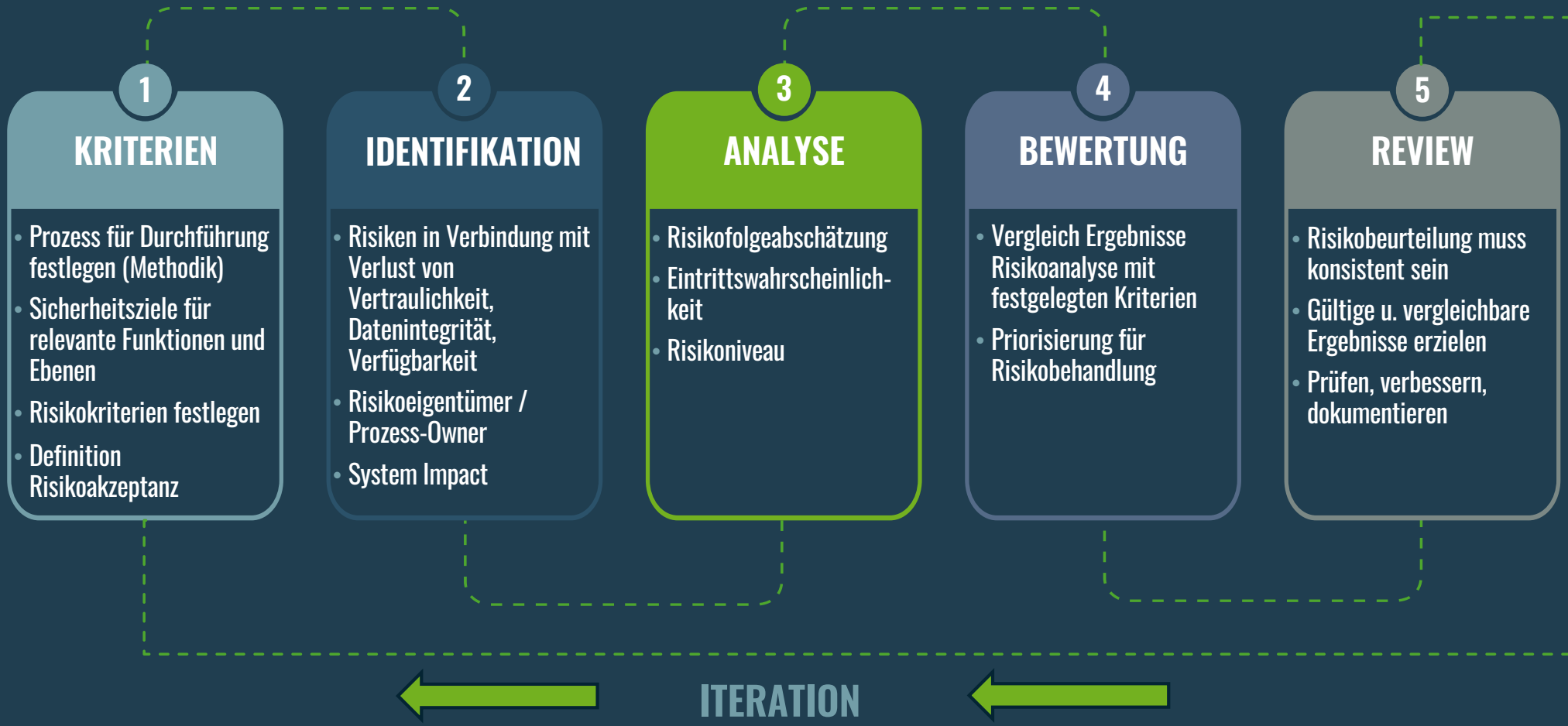
Bewertung der Risiken auf Basis von Produktqualität, Datenintegrität und ggf. Verbraucherschutz



Der Risikomanagementprozess sollte in Aufwand und Form sowie der Art der Dokumentation dem Risiko entsprechen

RISIKO-ADÄQUAT

RISIKOMANAGEMENT - RISIKOBEURTEILUNG



TECHNISCHE SICHERHEITSMAßNAHMEN

Foto von Victor Freitas auf Pexels

- ✓ Zugangskontrollen und Authentifizierung
- ✓ Audit Trails
- ✓ Datensicherung und Backups
- ✓ Datenverschlüsselung
- ✓ Validiertes und automatisiertes Data-Handling

ORGANISATORISCHE SICHERHEITSMAßNAHMEN

Foto von Gerd Altmann auf Pixabay

- ✓ Mitarbeiter-Schulungen und -sensibilisierung
- ✓ Zugriffsrechte
- ✓ Richtlinien für den sicheren Umgang mit Daten
- ✓ Kontinuierliche Risikoanalyse
- ✓ Audits und Überprüfungen

PROZESSUALE SICHERHEITSMAßNAHMEN

Foto von Tima Miroshnichenko auf Pexels

- ✓ Standardarbeitsanweisungen (SOPs)
- ✓ QM-System
- ✓ Gerätequalifizierung und Kalibrierung
- ✓ Protokolle zur Datensicherung und Wiederherstellung
- ✓ Computerized System Validation

COMPUTERSYSTEME – VALIDIERUNG (1)

KRITIKALITÄT

Auswirkungen auf kritische Funktionen

RISIKO

Anfälligkeit von Daten

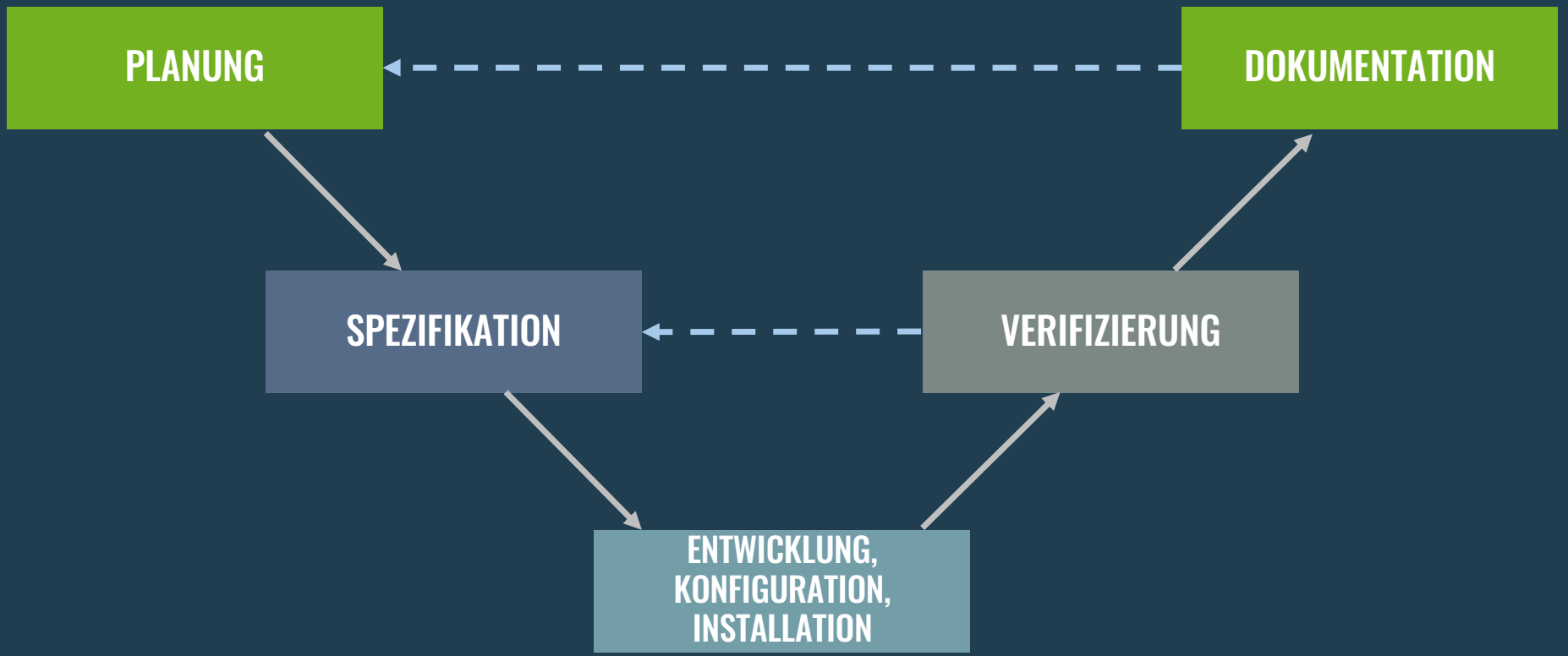
KOMPLEXITÄT

Hardware, Software, Schnittstellen, Benutzer

COMPUTERSYSTEME – VALIDIERUNG (2)

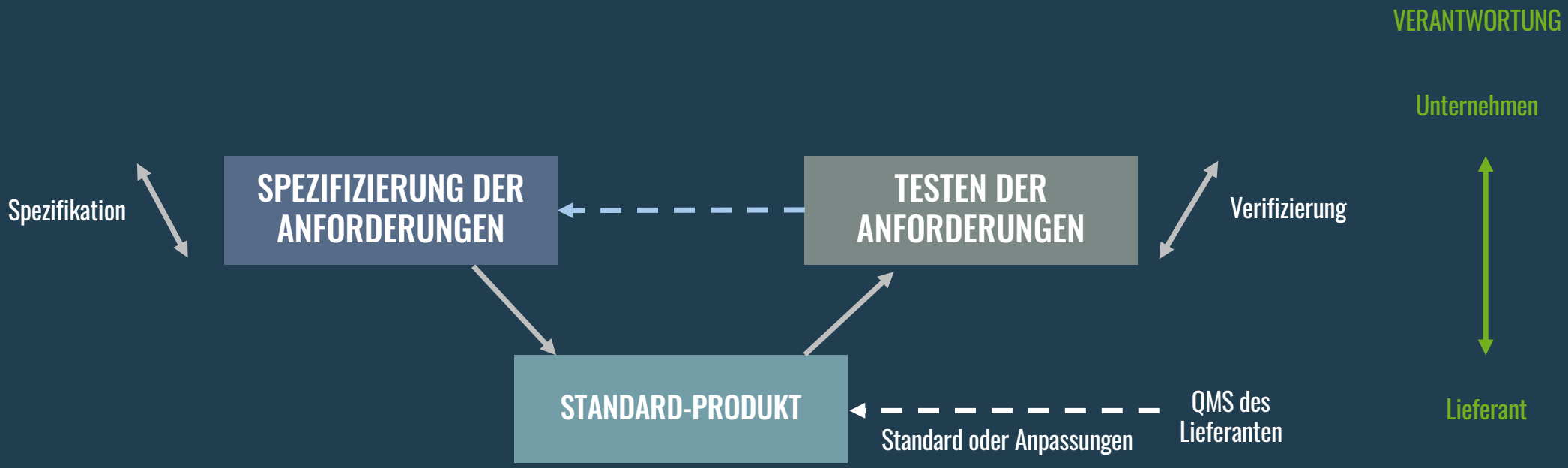
PLANUNG DURCHFÜHRUNG DOKUMENTATION

COMPUTERSYSTEME – VALIDIERUNG (3)



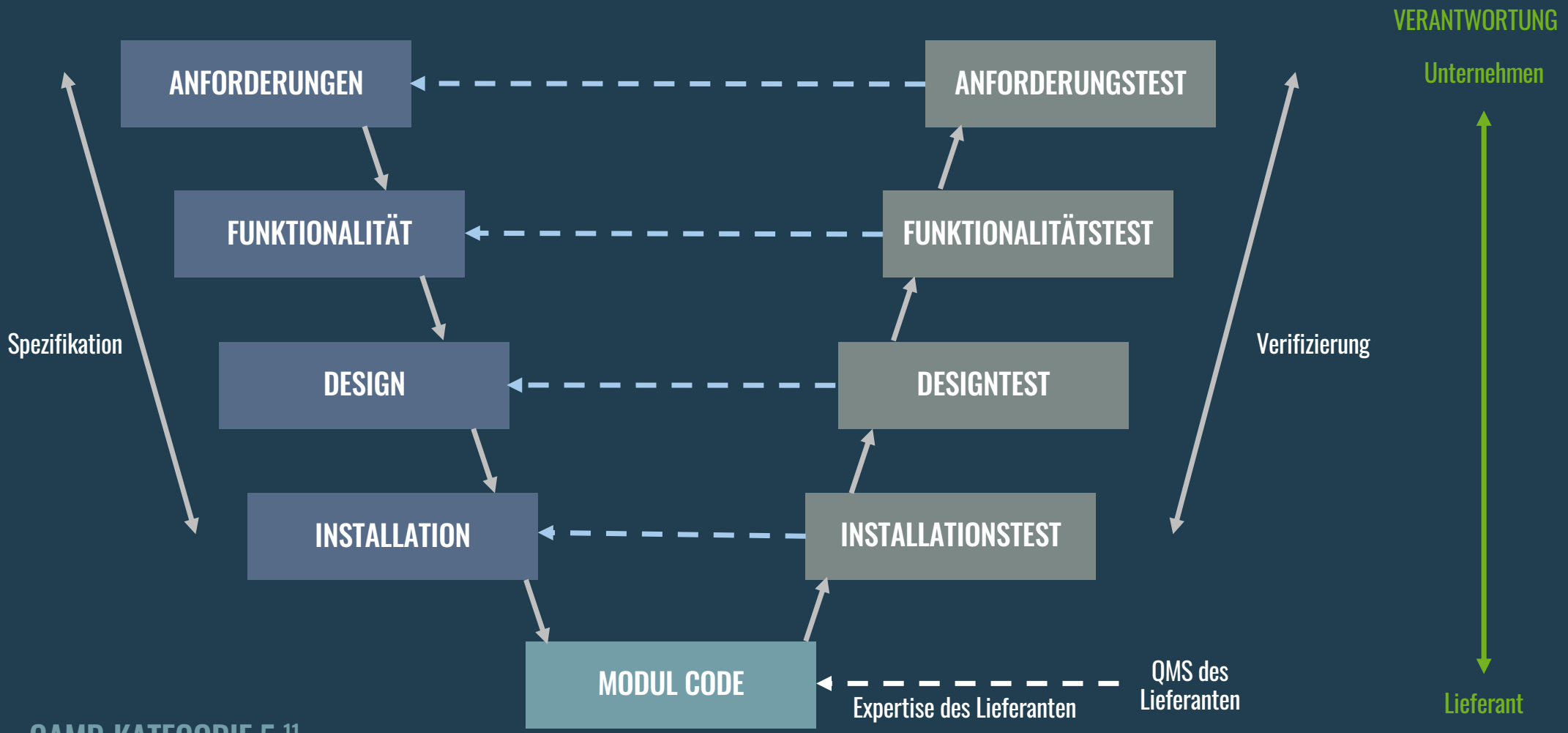
ALLGEMEINER VALIDIERUNGSANSATZ

COMPUTERSYSTEME – VALIDIERUNG (STANDARD-PRODUKT)



GAMP-KATEGORIE 3 [11]

COMPUTERSYSTEME – VALIDIERUNG (KUNDENSPEZIFISCHE APPLIKATION)



FAZIT

	VORTEILE	NACHTEILE
1 ÖKONOMISCH	• Kosteneinsparung durch Fehlervermeidung • Risikominimierung von Haftungsfällen • Steigerung Wettbewerbsfähigkeit • Effizientere Nutzung von Ressourcen	• Hohe Implementierungskosten • Laufende Wartungs- und Schulungskosten • Kosten für externe Audits und Beratung
2 PROZESSUAL	• Verbesserte Arbeitsprozesse und -effizienz • Schnelle Identifikation und Behebung von Fehlerquellen • Optimierte Dokumentations- und Nachweissysteme • Verlässliche und wiederholbare Testergebnisse • Effiziente Audit- und Inspektionsvorbereitung	• Erhöhter administrativer Aufwand • Längere Durchlaufzeiten • Komplexität in der Prozessgestaltung
3 SONSTIGES	• Höhere Kundenzufriedenheit und Vertrauensbildung • Erfüllung gesetzlicher u. regulatorischer Anforderungen • Positive Reputation uns Marktpositionierung • Förderung der Qualitätskultur im Unternehmen • Zukunftssicherheit und Innovationsfähigkeit	• Mitarbeiterunzufriedenheit • Potentielle Innovationshemmung • Einschränkung in der Flexibilität

REFERENZEN

[1] WHO Technical Report Series 996, Annex 5 - Guidance on Good Data and Record Management Practices, 2016

[2] MHRA Medicines and Healthcare products Regulatory Agency: 'GXP' Data Integrity Guidance and Definitions, March 2018

[3] U.S. FDA – U.S. Department of Health and Human Services, Food and Drug Administration: Data Integrity and Compliance with Drug cGMP, Q&A, Guidance for Industry, 2018

[4] PIC/S Guidance PI 041-1: Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments, Pharmaceutical Inspection Convention / Pharmaceutical Inspection Co-Operation Scheme, 2021

[5] DIN EN ISO/IEC 17025:2018-03: Allgemeine Anforderung an die Kompetenz von Prüf- und Kalibrierlaboratorien

[6] ISPE GAMP®: Records and Data Integrity Guide; International Society for Pharmaceutical Engineering, 2017

[7] ISPE Cultural Excellence Report – Six Key Dimensions; April 2017

[8] AMWHV Arzneimittel- und Wirkstoffherstellungsverordnung - Verordnung über die Anwendung der Guten Herstellungspraxis bei der Herstellung von Arzneimitteln und Wirkstoffen und über die Anwendung der guten fachlichen Praxis bei der Herstellung von Produkten menschlicher Herkunft; Stand 09.08.2019

[9] ICH International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use

[10] EMA Guideline on computerised systems and electronic data in clinical trial, EMA/INS/GCP/112288/2023, Good Clinical Practice Inspectors Working Group (GCP IWG), 09. März 2023

[11] ISPE GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems, Second Edition; International Society for Pharmaceutical Engineering, 2022

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT !

Carsten Schaffors
Remnitzhof 6
31177 Harsum
Fon: +49 172 707 0430
eMail: kontakt@imis-consulting.com
Web: imis-consulting.com

imis consulting

INTERIM MANAGEMENT & INDUSTRIAL SUPPORT