EBNER STOLZ

EIN Managementsystem für Informationssicherheit, Datenschutz, GoBD und vieles mehr

Ganzheitliche Managementsysteme

9. November 2021

A member of Nexia International

Inhaltsverzeichnis

1 Ausgewählte Compliancenormen - Kurzvorstellung und aktuelle Entwicklung 3

2 Viele Anforderungen - Ein Ziel 26

3 Das Managementsystem - Potenziale erkennen und Bereiche mehrfach nutzen 34

4 Fragen 37

© Ebner Stolz

Gliederung

Inhaltsverzeichnis

1 **Ausgewählte Compliancenormen - Kurzvorstellung und aktuelle Entwicklung** **3**

2 Viele Anforderungen - Ein Ziel 26

3 Das Managementsystem - Potenziale erkennen und Bereiche mehrfach nutzen 34

4 Fragen 37

© Ebner Stolz

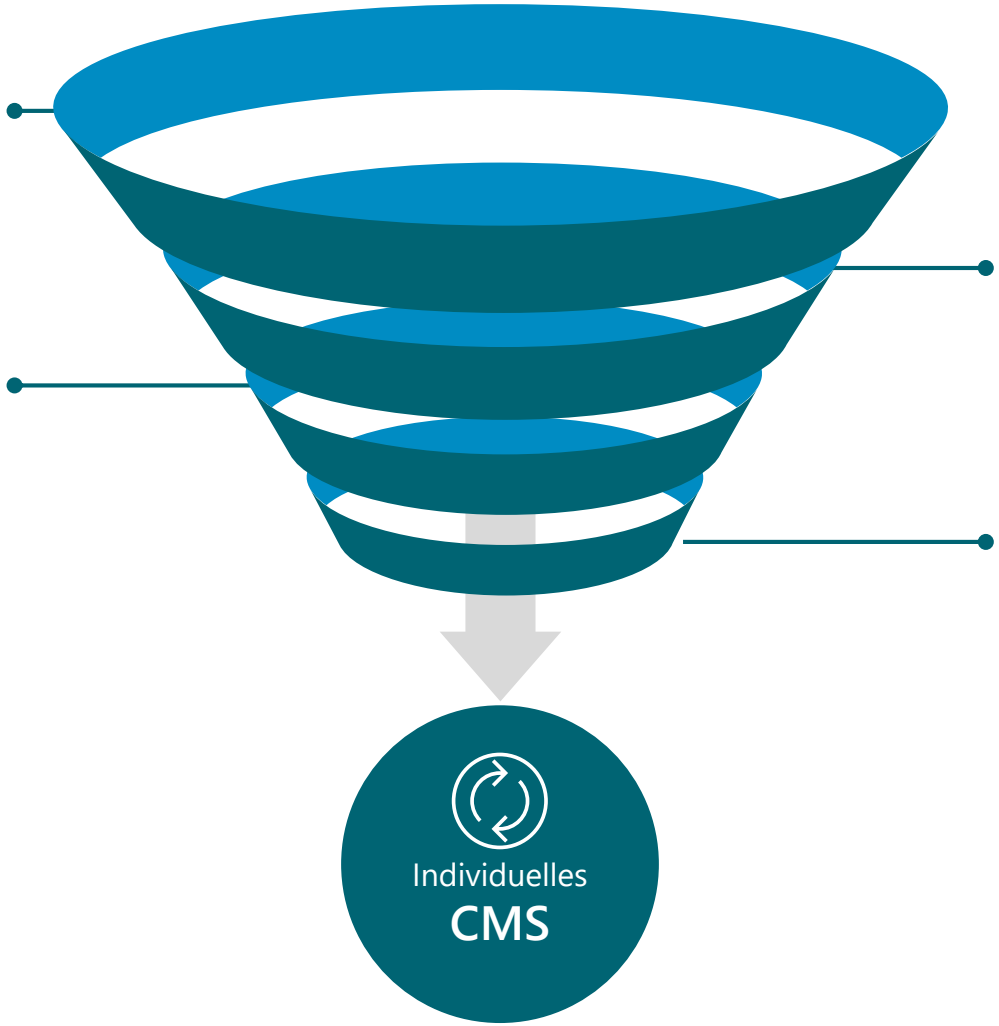
Die Treiber der einzelnen Managementsysteme

1 Unterschiedlichste Compliancegebiete
(Informationssicherheit, KRITIS, IT-SiG, Datenschutz, ...)

2 Identifikation, Bewertung und Steuerung von Risiken

3 Absicherung der Prozesse und Anforderungserfüllung
(Internes Kontrollsystem/ SOX/ ...)

4 Umsetzung und Überwachung der Maßnahmen



© Ebner Stolz

Was heißt das konkret?

*CMS = **C**ompliance **M**anagement**s**ystem

Extern: Regulatorisch

- BAIT/KAIT/, …
- HGB, StGB, AktG, GoBD, DSGVO, etc.
- Branchenspezifische Regelungen

Extern: Stakeholder

- Lieferanten
- Wettbewerber
- Kunden
- Mitarbeiter

Intern: Intrinsische Motivation

- Risk Management
- Compliance Management

Extern/Intern: Best Practice

- Erhöhung technische Sicherheit
- Erhöhung organisatorische Sicherheit

Summa summarum bleibt jeder Organisation nur übrig, eine Anforderungs- und Umfeldanalyse zu betreiben.

© Ebner Stolz

HABEN SIE EIN COMPLIANCE-MANAGEMENTSYSTEM?

> EINS? WIR HABEN SOGAR FÜNF!

Das ganzheitliche Managementsystem

1. PROZESS

- einheitliches und strukturiertes Vorgehen ist definiert und implementiert
- Integration weiterer Compliancegebiete möglich

2. COMPLIANCEANFORDERUNGEN

- Sollmaßnahmenkatalog ist vorhanden
- individuelle (unternehmensspezifische) Anforderungen sind erstellt
- Überschneidungen zwischen Normen werden erkannt
  (“erstelle einmal, verwende oft”)

4. ABSICHERUNG

- Internes Kontrollsystem als Umsetzungsnachweis und als Mittel zur Überwachung sind implementiert und werden gelebt
- Wiederverwenden von Kontrollen möglich

3. RISIKOMANAGEMENT

- einheitliches und strukturiertes Risikomanagement ist umgesetzt
- Integration von Risiken “außerhalb” des Managementsystems möglich

Verschiedene Compliancenormen mit dem Ziel, die Sicherheit zu erhöhen

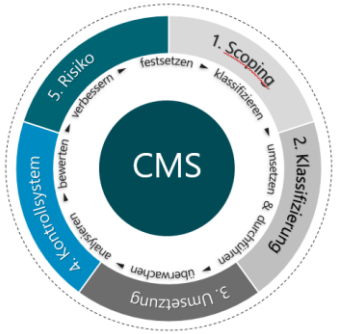
1. IT-SICHERHEITSGESETZ/ KRITISCHE INFRASTRUKTUREN (KRITIS)

2. BANKAUFSICHTLICHE ANFORDERUNGEN AN DIE IT (BAIT)

3. TISAX

4. KRANKENHAUS-ZUKUNFTSGESETZ (KHZG)/PDSG)

5. UMWELTMANAGEMENT/ SOCIAL RESPONSIBILITY



© Ebner Stolz

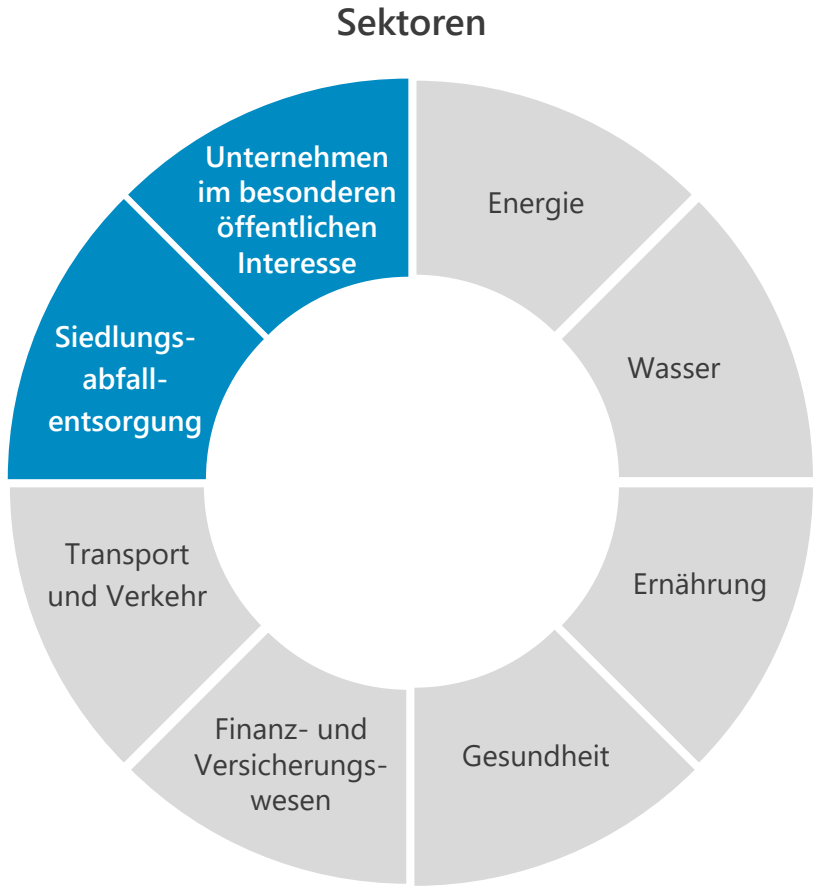
1. IT-Sicherheitsgesetz 2.0, kritische Strukturen oder doch Komponenten?

Das Wichtigste im Überblick

- Das IT-Sicherheitsgesetz 2.0 ist am 28. Mai 2021 in Kraft getreten
- Bereits im April und Mai 2021 wurde es von Bundesrat und Bundestag beschlossen (19/28844)

- Die neue KRITIS-Verordnung 2.0 senkt einige Schwellenwerte und ergänzt und ändert die KRITIS-Anlagen 2.0
- Die „Zweite Verordnung zur Änderung der BSI-KRITIS Verordnung" tritt zum 1.1.2022 in Kraft

- Erweiterung der bisherigen Sektoren um Siedlungsabfallentsorgung sowie Unternehmen im besonderen öffentlichen Interesse (UBI)
  - UB1: Unternehmen, „die Güter nach § 60 Absatz 1 Nummer 1 und 3 der Außenwirtschaftsverordnung"
  - UB2: Unternehmen, „die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind"
  - UB3: Betreiber „eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung in der jeweils geltenden Fassung" oder Betreiber, die, „nach § 1 Absatz 2 der Störfall-Verordnung diesen gleichgestellt sind"



© Ebner Stolz

1. IT-Sicherheitsgesetz 2.0, kritische Strukturen oder doch Komponenten?

ANGRIFFSERKENNUNG

- Ab 1. Mai 2023 Einsatz von Systemen zur Angriffserkennung notwendig
- Systeme zur Angriffserkennung sind durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse
- **Einsatz von SIEM/SOC-Lösungen**

KRITISCHE KOMPONENTEN

- Komponenten, die z. B. in Kritischen Infrastrukturen eingesetzt werden
- Der Ausfall der Komponenten würde eine KRITIS-Anlage erheblich beeinträchtigen
- Garantieerklärung
- Müssen pro Sektor in den jeweiligen Gesetzen definiert werden
- Für Telekommunikation bereits erfolgt

LIEFERKETTEN

- Garantieerklärung erstreckt sich auf die gesamte Lieferkette des Herstellers
- Erweiterung der Risikoanalyse notwendig, da auch Aspekte, wie Spionage, Sabotage und Terrorismus, betrachtet werden müssen

UMSETZUNG STATT BUßGELD

Der Bußgeldrahmen erhöht sich auf 2 Mio. EUR. Durch den Verweis auf § 30 Abs. 2 Satz 3 OWiG kann sich die Bußgeldhöhe auf bis zu 20 Mio. Euro verzehnfachen.

Risiken identifizieren
Anforderungen umsetzen

© Ebner Stolz

2. Bankaufsichtliche Anforderungen an die IT (BAIT)

© Ebner Stolz

2. Bankaufsichtliche Anforderungen an die IT (BAIT)

BAIT	VAIT	KAIT	ZAIT
› Erstveröffentlichung am 6. November 2017 › Aktualisierung zum 14. September 2018 – Aufnahme „KRITIS“ › BAIT Neu seit 16. August 2021	› Erstveröffentlicht am 2. Juli 2018 › Aktualisierung zum 20. März 2019 – Aufnahme „KRITIS“ › Eröffnung der Konsultation zum 17. August 2021	› Erstveröffentlichung am 1. Oktober 2019	› Erstveröffentlichung am 16. August 2021

Die neue Fassung der BAIT wurde am 16. August 2021 veröffentlicht und ist **am selben Tag in Kraft getreten!**

© Ebner Stolz

2. Bankaufsichtliche Anforderungen an die IT (BAIT) - Informationsrisikomanagement

Aus BAIT Neu Tz. 3.7.

„Das Institut hat auf Basis der festgelegten Risikokriterien einen **Vergleich der Sollmaßnahmen mit den jeweils wirksam umgesetzten Maßnahmen (Ist-Zustand)** durchzuführen."

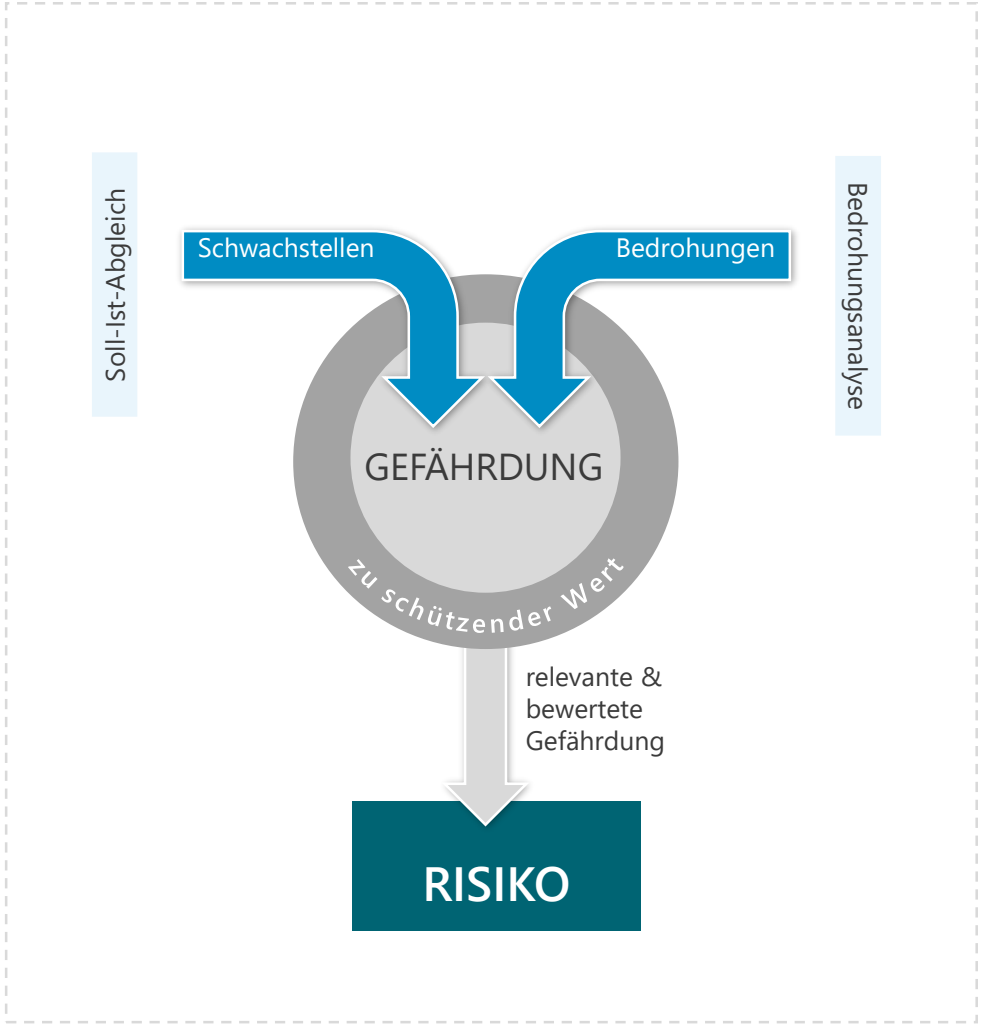
„Die Risikoanalyse berücksichtigt über den Soll-Ist-Vergleich hinaus u. a. mögliche Bedrohungen, das Schadenspotenzial, die Schadenshäufigkeit sowie den Risikoappetit. Sonstige risikoreduzierende Maßnahmen können hierbei berücksichtigt werden. Falls Soll-Maßnahmen nicht implementiert werden können, z. B. aufgrund technischer Restriktionen, können sonstige risikoreduzierende Maßnahmen umgesetzt werden."

Aus BAIT Neu Tz. 3.8.

„Sonstige risikoreduzierende Maßnahmen aufgrund unvollständig umgesetzter Soll-Maßnahmen sind wirksam zu koordinieren, zu dokumentieren, zu überwachen und zu steuern."

Maßnahmen

- prozessual sicherstellen, dass Schadenspotential, Schadenshäufigkeit und Risikoappetit im Rahmen der Risikoanalyse berücksichtigt werden
- Implementierung eines geregelten Prozesses zum Umgang mit risiko-reduzierenden Maßnahmen



© Ebner Stolz

2. Bankaufsichtliche Anforderungen an die IT (BAIT) - Informationsrisikomanagement

Aus BAIT Neu Tz. 4.8

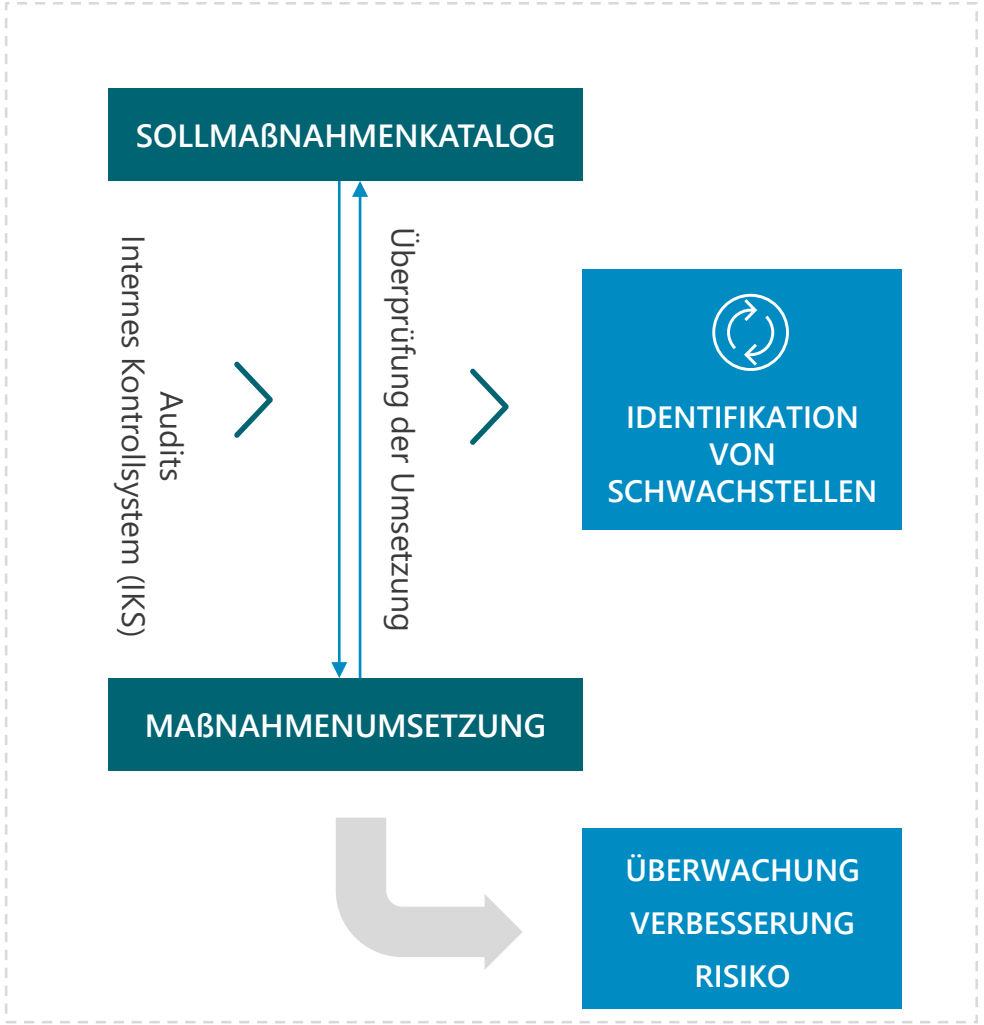
„Das Institut hat eine Richtlinie über das Testen und Überprüfen der Maßnahmen zum Schutz der Informationssicherheit einzuführen und diese regelmäßig und anlassbezogen zu überprüfen und bei Bedarf anzupassen."

„Die Richtlinie berücksichtigt u. a.:

- die allgemeine Bedrohungslage
- die individuelle Risikosituation des Instituts
- Kategorien von Test- und Überprüfungsobjekten (z. B. das Institut, IT-Systeme, Komponenten)
- die Art, Umfang und Frequenz von Tests und Überprüfungen
- Zuständigkeiten und Regelungen zur Vermeidung von Interessenskonflikten."

Maßnahmen

- Erstellung einer Richtlinien mit Vorgaben zum Testen und Überprüfen der Maßnahmen zum Schutz der Informationssicherheit. Hierbei sollten zumindest die aufgeführten Inhalte berücksichtigt werden. Gleichzeitig ist die Richtlinie in die Review-Prozesse für das Anweisungswesen einzubinden.
- Erstellung eines Audit- und Kontrollplans auf Basis der Richtlinie.



© Ebner Stolz

3. TISAX – bin ich denn schon gelabelt oder was?

Die Grundlagen

- Der Verband der Automobilindustrie (VDA) hat zur Sicherstellung eines angemessenen Niveaus zur Informationssicherheit bei Lieferanten und Dienstleistern im Automobilbereich ein Prüf- und Austauschverfahren entwickelt.
- Es handelt sich dabei um einen entwickelten Fragebogen zur Informations-sicherheit, dem „Information Security Assessment“ (ISA); alles besser bekannt unter dem Namen TISAX (Trusted Information Security Assessment eXchange).
- Mit dem VDA ISA will die Automobilindustrie das wachsende Sicherheitsbedürfnis zwischen OEMs (Original Equipment Manufacturer) und Lieferanten im Umgang mit vertraulichen Informationen adressieren.
- Kurz gesagt: Keine Zusammenarbeit ohne TISAX-Label

Der Aufbau

- basiert auf zwei internationalen Normen: ISO 27001 für Informationssicherheits-Managementsysteme (ISMS) und ISO 27017 für Cloud Sicherheit
- Wird erweitert um Vorgaben für Prototypenschutz

INFORMATIONS-SICHERHEIT IN DER AUTOMOBIL-INDUSTRIE

Ein einheitliches Sicherheitsniveau als gemeinsames Ziel

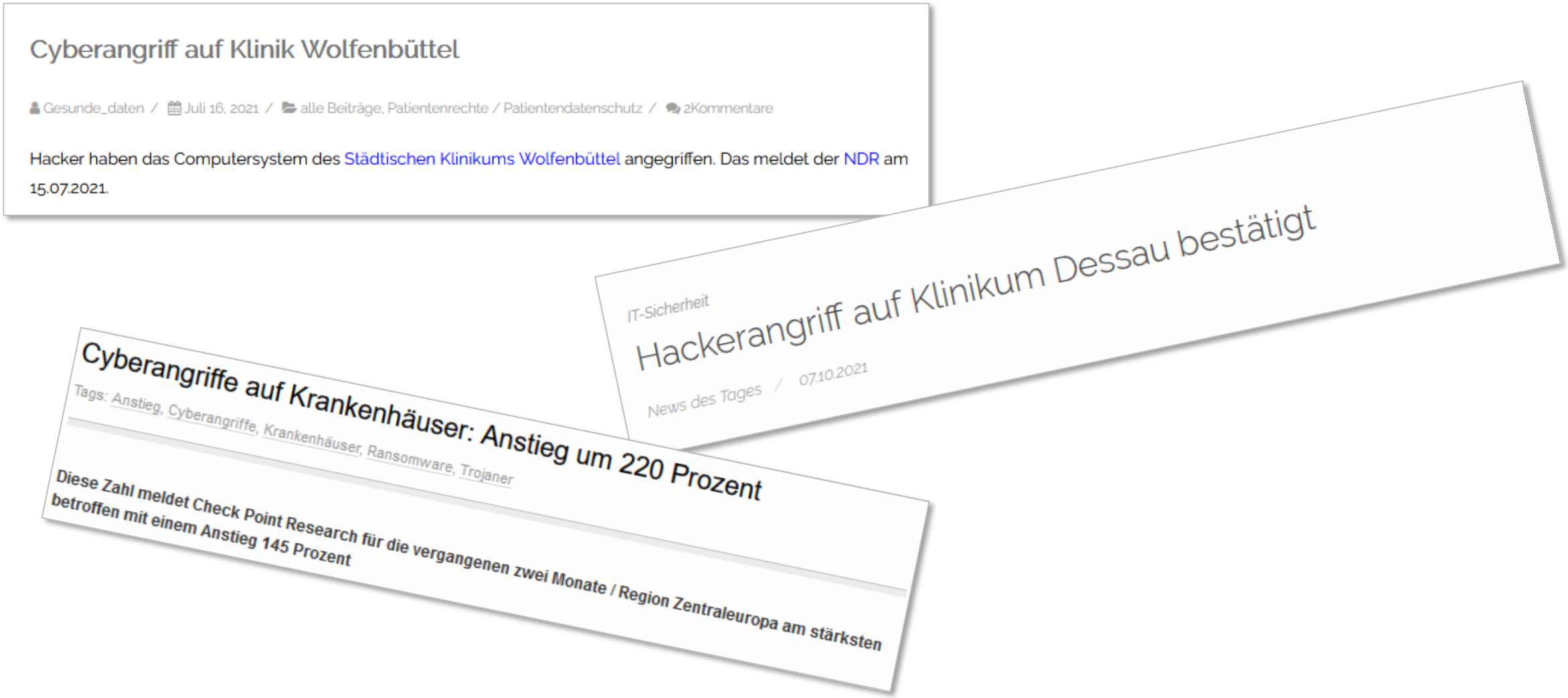
▼

Risiken identifizieren Anforderungen umsetzen

Umsetzung überwachen & verbessern (Reifegrade)

© Ebner Stolz

4. Krankenhauszukunftsgesetz (KHZG)/Patientendatenschutzgesetz (PDSG)



4. Krankenhauszukunftsgesetz (KHZG)/Patientendatenschutzgesetz (PDSG)

1. Krankenhäuser sind ein exponiertes Ziel

- Zeitdruck in der operativen Arbeit
- Patientendaten
- Vielfältiger Mailkontakt (Lieferanten, Kunden, Versicherungen, Ärzte, andere Kliniken; insgesamt viele unbekannte Absender von E-Mails, welche bearbeitet werden müssen)
- Cyberkriminelle konzentrieren sich in Corona-Zeiten besonders auf kritische Infrastruktur, um möglichst viel Schaden anzurichten. Mittlerweile vermehrt Ziel von Hackerangriffen

2. „Kein Gefühl für Gefahr"

- Die Belegschaft besaß keine ausreichende Sicherheits-Awareness
- Das Pflege- und Personalmangel steigert die Gefahr

3. Unzureichende Maßnahmen

- Mit dem Digitalisierungsschub durch die Pandemie gehen neue Möglichkeiten für Angriffe einher
- Schutzmechanismen sind nicht „State of the Art"
- Krankendaten als lukratives Gut auf dem Schwarzmarkt
- Die Frage nach der Datensicherung in einer vernetzten Welt: Spionage und Verschlüsselung

4. Kein Management

- Es lässt sich festhalten, dass kein Management der IT-Sicherheit, aber vor allem kein Management der Informationssicherheit, bestand
- Ein reines IT-Sicherheitsmanagement hätte die Situation ebenfalls nicht verhindern können
- Es braucht einen **ganzheitlichen, lebbaren Ansatz**

Risiken identifizieren
Anforderungen umsetzen,
überwachen, verbessern

© Ebner Stolz

4. Krankenhauszukunftsgesetz (KHZG)/Patientendatenschutzgesetz (PDSG)

IT-Sicherheitsgesetz

- Pflicht zur Einhaltung von IT-Sicherheitsstandards (Stand der Technik) für definierte Sektoren (Gesundheitswesen)
- Informations-Sicherheits-Management-System (ISMS)
- Branchenstandard B3S beinhaltet die konkreten Anforderungen, die im Sinne des IT-SiG umzusetzen sind (Orientierung an ISO 27001)
- *Schwellenwert: 30.000 vollstationäre Behandlungsfälle*

Patientendatenschutzgesetz

- § 75 c) Sozialgesetzbuch V
- „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informations-technischen Systeme, Komponenten oder Prozesse“
- Frist bis 1. Januar 2022

Aufbau eines ganzheitlichen ISMS

Vermeidung von Störungen der informationstechnischen Systeme, insbesondere mit Blick auf die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der IT-Systeme und Daten.

© Ebner Stolz

5... und es muss auch nicht immer IT sein
Vom Umweltmanagement bis hin zur Corporate Social Responsibility

UMWELTMANAGEMENT (ISO 14001)

- Umweltschutz bereits von großer Bedeutung, Tendenz steigend
- Besondere Relevanz auch für interessierte Parteien (Gesetzgeber, Kunden, ...)
- Umweltbelastungen über den gesamten Lebensweg von Produkten und Dienstleistern reduzieren/vermeiden
- Reduzierung von Umweltrisiken
- Umweltziele definieren, Umweltaspekte berücksichtigen, Maßnahmen und Prozesse definieren und umsetzen, Wirksamkeit prüfen und verbessern

PDCA - ZYKLUS

Risiken identifizieren
Anforderungen umsetzen

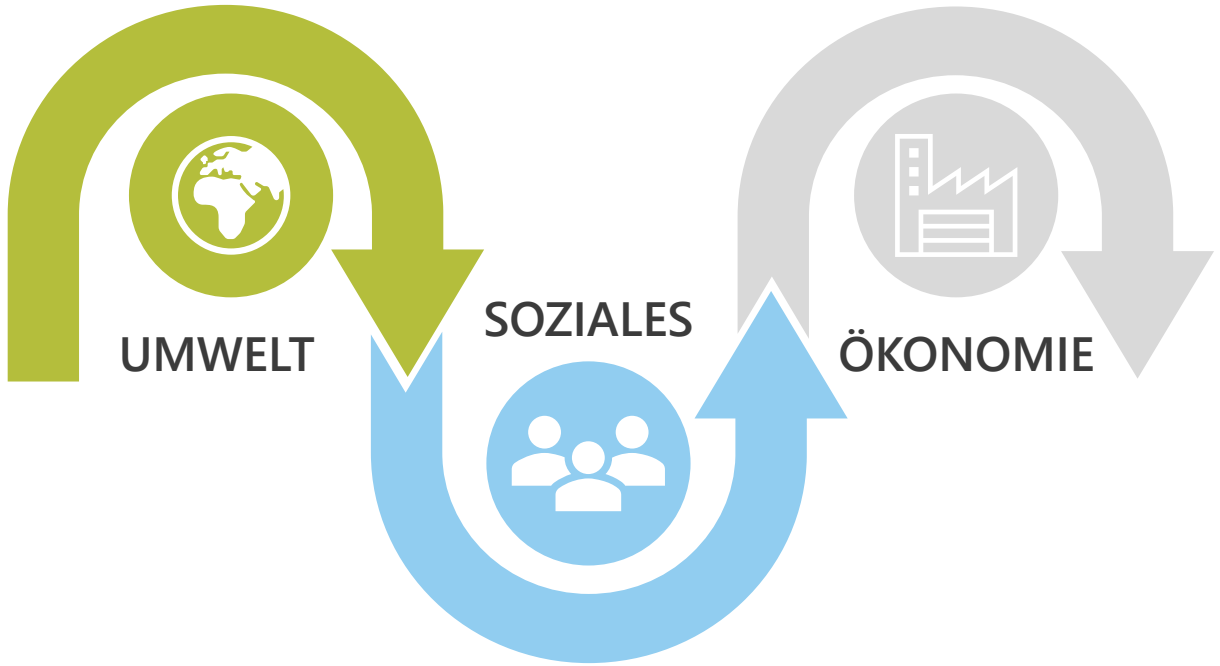
Umsetzung überwachen & verbessern

ENERGIEMANAGEMENT (ISO 50001)

- Verbesserung der energiebezogenen Leistungen (Folge z. B. Erhöhung der Energie-effizienz)
- Minderung des Energieverbrauchs und der damit verbundenen Treibhausgasemissionen
- Reduzierung von Energierisiken
- Definition Energiepolitik und Energieziele, Erstellung und Umsetzung von Maßnahmen und Aktionspläne, Prüfen der Wirksamkeit und der Zielerreichung

© Ebner Stolz

5... und es muss auch nicht immer IT sein
Vom Umweltmanagement bis hin zur Corporate Social Responsibility



- European Green Deal
- CSR- /Nachhaltigkeitsberichterstattung

CORPORATE SOCIAL RESPONSIBILITY (CSR)

- Themengebiete „Nachhaltigkeit“ und „soziale Verantwortung“ im Fokus
- Adressierung von Themenbereichen, wie Umwelt, Menschenrechte, Arbeitsbedingungen sowie faire Betriebs- und Geschäftspraktiken

Risiken identifizieren, Anforderungen umsetzen

Umsetzung überwachen & verbessern

© Ebner Stolz

Inhaltsverzeichnis

1 Ausgewählte Compliancenormen - Kurzvorstellung und aktuelle Entwicklung 3

2 Viele Anforderungen - Ein Ziel 26

3 Das Managementsystem - Potenziale erkennen und Bereiche mehrfach nutzen 34

4 Fragen 37

© Ebner Stolz

CMS – Das (altbekannte) grundlegende Vorgehen

ACT

- Verbesserungsmaßnahmen
- Umgang mit Abweichungen (non-compliance)

PLAN

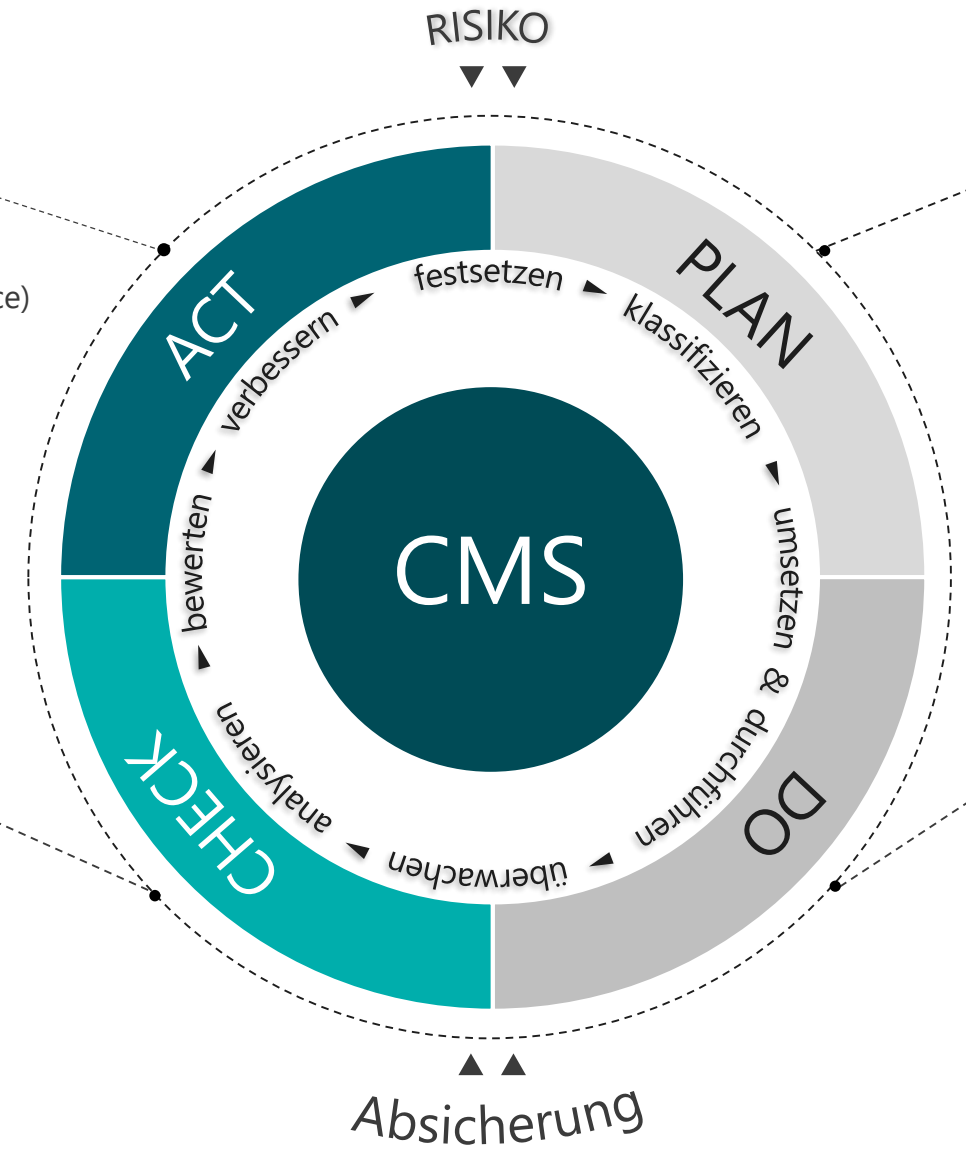
- Compliancegebiet(e) definieren
- Ziele und Grundsätze
- Rollen & Verantwortlichkeiten
- Risiken

CHECK

- Wirksamkeit messen und prüfen
- Kontinuierliches Monitoring
- Durchführen Interner Audits

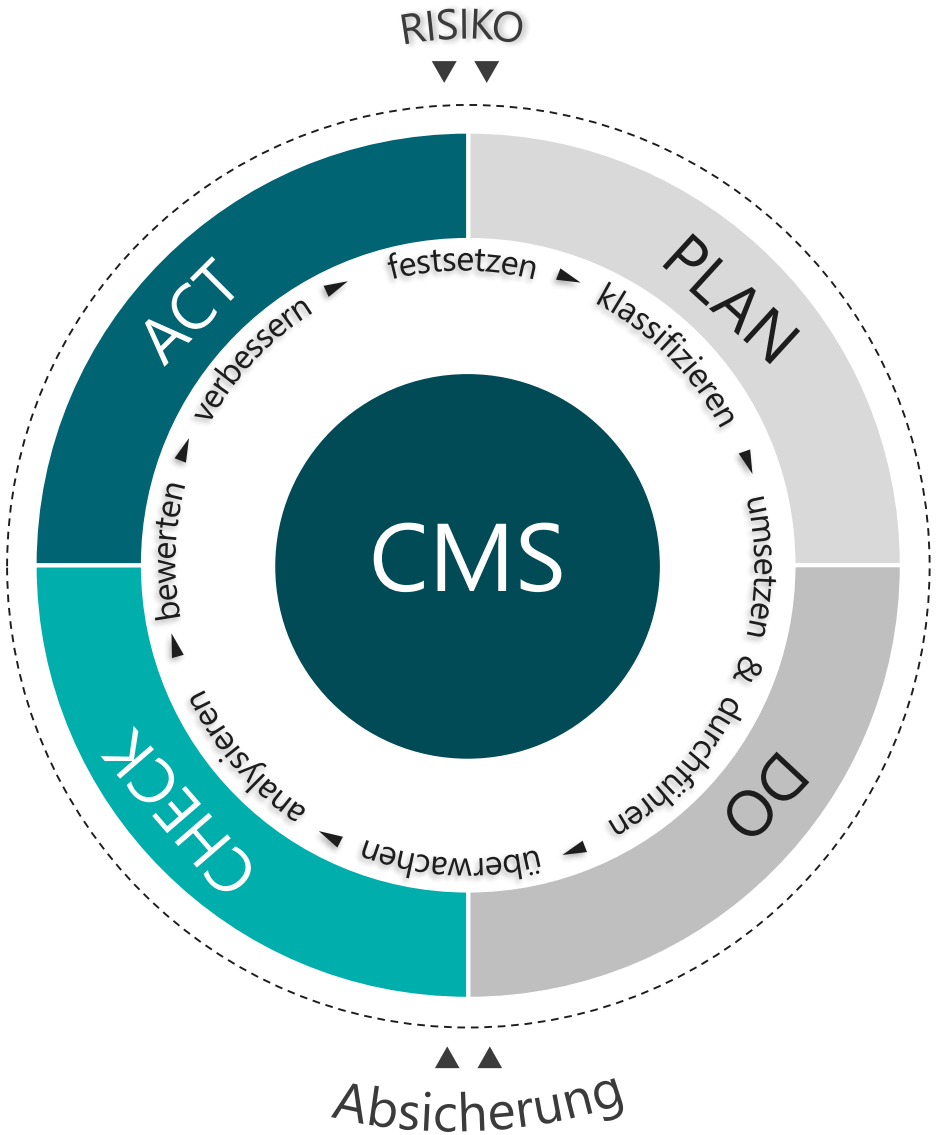
DO

- Umsetzung & Steuerung
- Kommunikation & Schulung
- Dokumentation & Betrieb



© Ebner Stolz

ISO 37301 – Compliance-Managementsysteme



Alles NEU macht die ISO 37301

- Die ISO 37301:2021 definiert die Anforderungen an den Aufbau, die Umsetzung und Wirksamkeitskontrolle eines Compliance-Management-Systems.
- Sie ersetzt die ISO 19600 aus dem Jahre 2014
- Sie wurde am 13. April 2021 veröffentlicht und ist damit in Kraft getreten
- Sie unterscheidet sich kaum von der ISO 19600

- Nun als **A-Norm zertifizierbar**
- Bei Orientierung an die ISO 19600 oder den IDW PS 980 sind keine großen Anpassungen an ein bestehendes CMS zu erwarten

© Ebner Stolz

Das ganzheitliche Managementsystem

1. PROZESS

- einheitliches und strukturiertes Vorgehen ist definiert und implementiert
- Integration weiterer Compliancegebiete möglich

2. COMPLIANCEANFORDERUNGEN

- Sollmaßnahmenkatalog ist vorhanden
- individuelle (unternehmensspezifische) Anforderungen sind erstellt
- Überschneidungen zwischen Normen werden erkannt
  (“erstelle einmal, verwende oft”)

4. ABSICHERUNG

- Internes Kontrollsystem als Umsetzungsnachweis und als Mittel zur Überwachung sind implementiert und werden gelebt
- Wiederverwenden von Kontrollen möglich

3. RISIKOMANAGEMENT

- einheitliches und strukturiertes Risikomanagement ist umgesetzt
- Integration von Risiken “außerhalb” des Managementsystems möglich

Gliederung

Inhaltsverzeichnis

1 Ausgewählte Compliancenormen - Kurzvorstellung und aktuelle Entwicklung 3

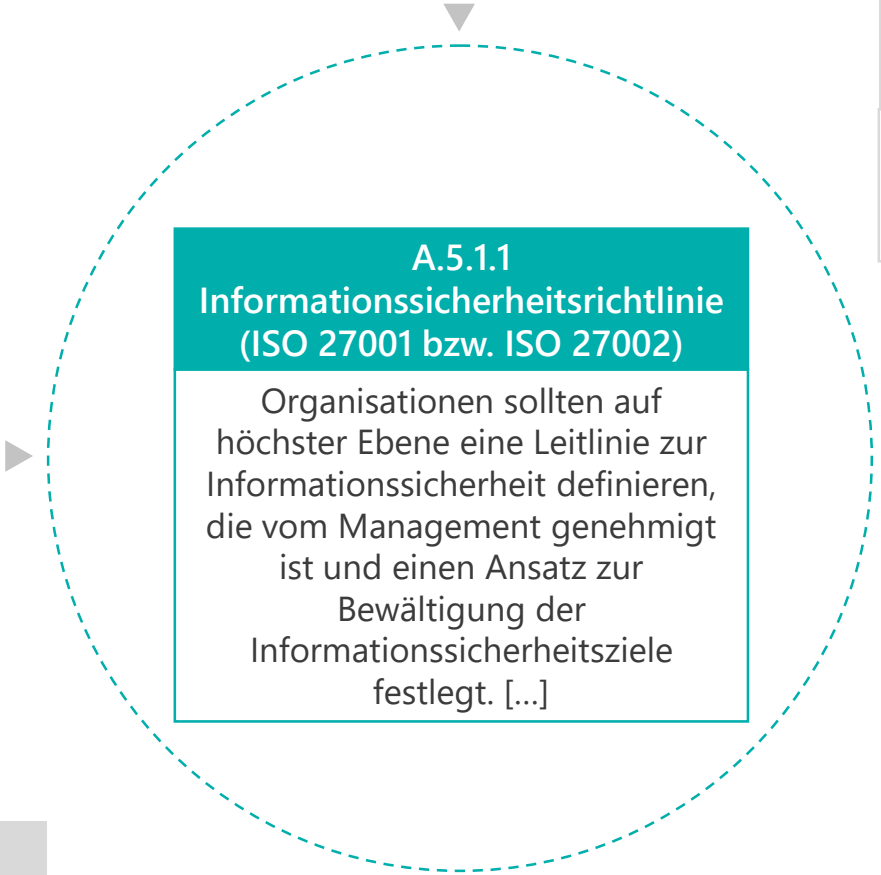
2 Viele Anforderungen - Ein Ziel 26

3 Das Managementsystem - Potenziale erkennen und Bereiche mehrfach nutzen 34

4 Fragen 37

© Ebner Stolz

Der Überschneidungscharakter der einzelnen Compliancenormen



Datenschutz-Grundverordnung (Art. 32)

[...] treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. [...]

4. Informationssicherheits-management (BAIT Tz. 4.2)

Die Geschäftsleitung hat eine Informationssicherheitsleitlinie zu beschließen und innerhalb des Instituts zu kommunizieren. [...]

2.4 Sicherheitsleitlinie (B3S Lebensmittelhandel)

Eine Umsetzung der Sicherheitsleitlinie findet durch die einzelnen Richtlinien für IT- und Informationssicherheit statt. [...]

A.5.1.1 Informationssicherheitsrichtlinie (ISO 27001 bzw. ISO 27002)

Organisationen sollten auf höchster Ebene eine Leitlinie zur Informationssicherheit definieren, die vom Management genehmigt ist und einen Ansatz zur Bewältigung der Informationssicherheitsziele festlegt. [...]

...

...

1.1 Information Security Policies (VDA ISA 1.1.1)

Die Organisation benötigt mindestens eine Richtlinie für Informationssicherheit. [...]

OIS-02 Leitlinie zur Informationssicherheit (BSI C5)

Die oberste Leitung des Cloud-Anbieters hat eine Leitlinie zur Informationssicherheit verabschiedet und an die internen und externen Mitarbeiter sowie die Cloud-Kunden kommuniziert. [...]

CC1.4 Control Environment (SOC2)

Establishes Policies and Practices - Policies and practices reflect expectations of competence necessary to support the achievement of objectives. [...]

© Ebner Stolz

Das ganzheitliche Managementsystem

1. PROZESS

- einheitliches und strukturiertes Vorgehen ist definiert und implementiert
- Integration weiterer Compliancegebiete möglich

2. COMPLIANCEANFORDERUNGEN

- Sollmaßnahmenkatalog ist vorhanden
- individuelle (unternehmensspezifische) Anforderungen sind erstellt
- Überschneidungen zwischen Normen werden erkannt
  (“erstelle einmal, verwende oft”)

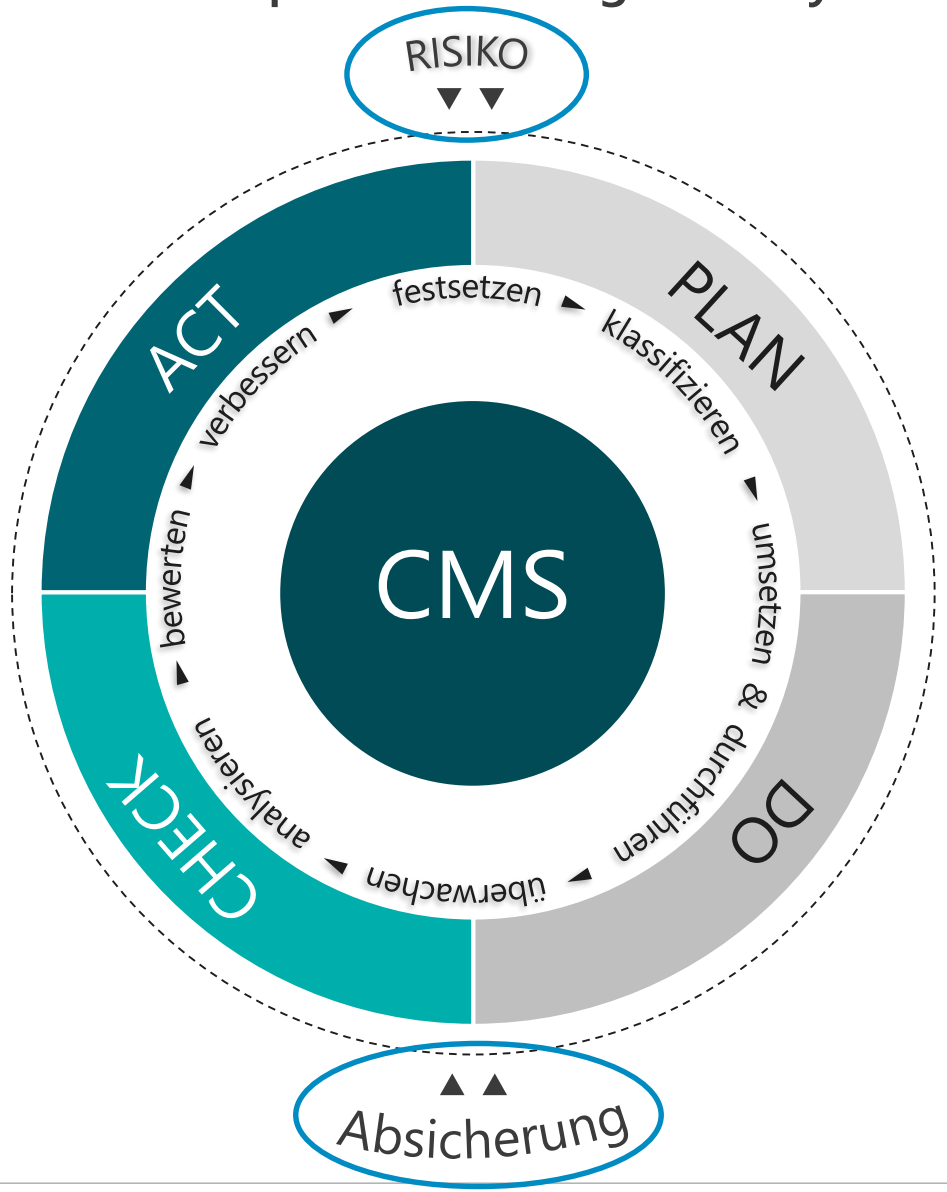
3. RISIKOMANAGEMENT

- einheitliches und strukturiertes Risikomanagement ist umgesetzt
- Integration von Risiken “außerhalb” des Managementsystems möglich

4. ABSICHERUNG

- Internes Kontrollsystem als Umsetzungsnachweis und als Mittel zur Überwachung sind implementiert und werden gelebt
- Wiederverwenden von Kontrollen möglich

ISO 37301 – Compliance-Managementsysteme



Alles NEU macht die ISO 37301

- Die ISO 37301:2021 definiert die Anforderungen an den Aufbau, die Umsetzung und Wirksamkeitskontrolle eines Compliance-Management-Systems (CMS)
- Sie ersetzt die ISO 19600 aus dem Jahre 2014
- Sie wurde am 13. April 2021 veröffentlicht und ist damit in Kraft getreten
- Sie unterscheidet sich kaum von der ISO 19600

- Nun als **A-Norm zertifizierbar**
- Bei Orientierung an die ISO 19600 oder den IDW PS 980 sind keine großen Anpassungen an ein bestehendes CMS zu erwarten

© Ebner Stolz

Risiken und Kontrollen im MS erweitern

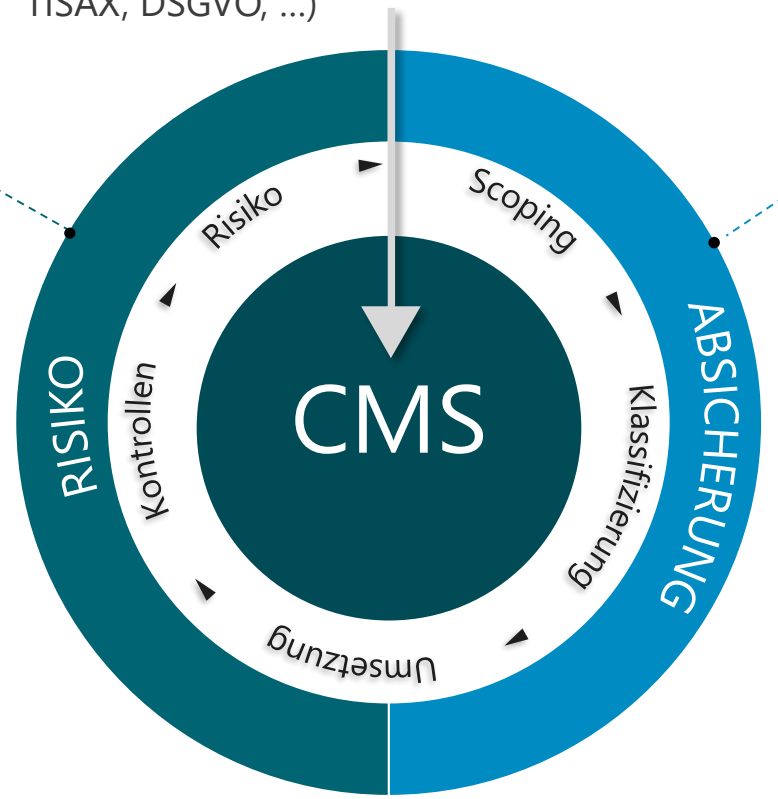
ANFORDERUNG

Identifizierte Anforderungen/Controls des Ziels CMS (z. B. ISO 27001, BAIT, Tax, GoBD, TISAX, DSGVO, ...)

RISIKO

Aufbau eines Risikomanagementsystems, das

- sowohl Risiken aus den jeweils zugrundeliegenden Compliancegebieten identifiziert, bewertet und überwacht als auch
- die Steuerung der übergreifenden Unternehmens- bzw. Compliancerisiken/Ad Hoc Risiken überwacht (z. B. KonTraG)



KONTROLLEN

Aufbau eines ganzheitlichen Internen Kontrollsystems (IKS), das

- über das typische interne Audit als alleiniges Mittel zur kontinuierlichen Verbesserung hinaus geht und
- somit eine Überwachung der Anforderungen auf allen Ebenen des CMS ermöglicht

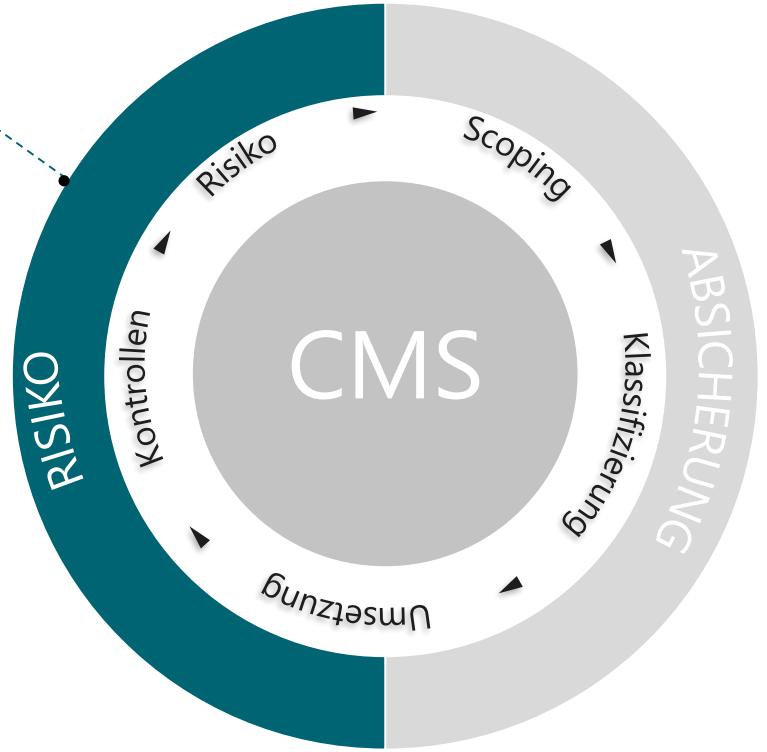
Maßnahmensteuerung und -überwachung

© Ebner Stolz

Das Thema „Risiko“

RISIKO

- Management steuerbarer Risiken in handhabbarer Anzahl (Fokussierung/Mapping)
- Risikomanagement trägt zur besseren Fundierung unternehmerischer Entscheidungen bei und unterstützt bei der Einhaltung der Compliance-gebiete

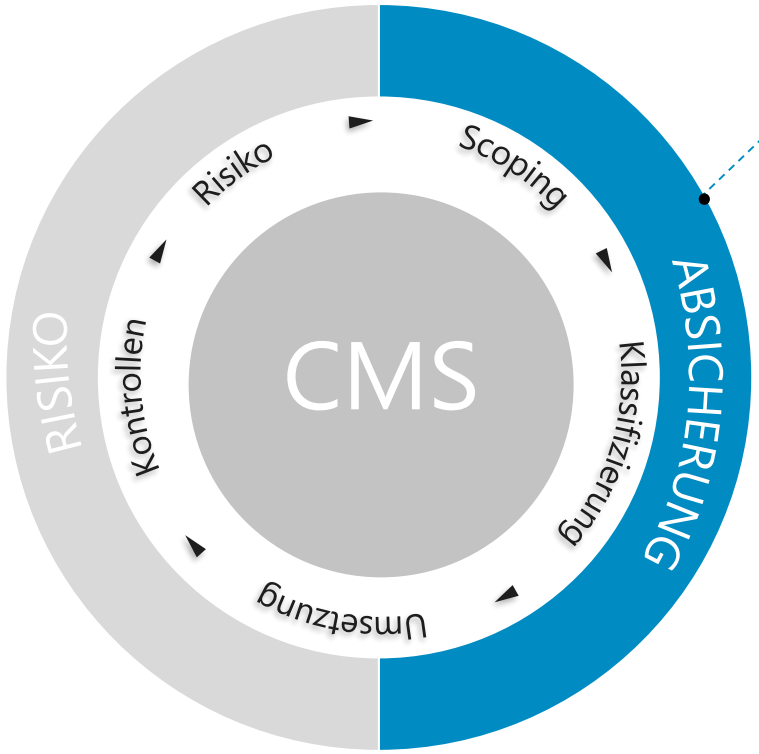


ERWEITERUNG DES RISIKOMANAGEMENTSYSTEMS

- **Erweiterung und Verknüpfung** des Risikomanagements um Bereiche „außerhalb“ des Managementsystems, z. B. um **KonTraG**
- Identifikation, Bewertung und Kommunikation **sämtlicher** im Unternehmen auftretenden Risiken, zumindest, wenn diese das Potenzial der Bestands-gefährdung aufweisen. Maßnahmen umsetzen, die Risiken verringern, übertragen oder vermeiden.

© Ebner Stolz

Mittels „IKS“ das Managementsystem „leben“



KONTROLLEN

- Nachweis zur Umsetzung der Anforderungen
- Frühzeitige Reaktion auf Abweichungen bei der Anforderungsumsetzung
- Risikoreduktion durch Kontrollen
- Kontrollen als Mehrwert, z. B. als Nachweis zur **IT-Prüfung im Rahmen der Jahresabschlussprüfung** (aber auf Scope achten)

VOM BSI C5 ZUM MANAGEMENTSYSTEM

- Das **Control Framework als Basis** für den initialen oder weiteren Aufbau eines Managementsystems - sofern identifizierte Kontrollziele (teilweise) mit Anforderungen eines Compliancemodells zusammenhängen (z. B. Anforderungen zur Informationssicherheit oder Datenschutz)
- Von der Kontrollseite ausgehend können **korrespondierende Anforderungen** aus dem relevanten Complianceumfeld adressiert und umgesetzt werden
- Vom ISAE 3XXX/SOC2/BSI C5 zum Managementsystem

© Ebner Stolz

Das Ganze mal umdrehen – Über Outsourcing/Cloud zum MS

- Outsourcing/Cloud Lösungen immer beliebter
- Trend setzt sich während Pandemie fort (Office 365, Google Suite,…)
- Aber: Dienstleister kontrollieren

- Muss Auftraggeber nachweisen können, dass Verarbeitung/ Dienstleistung/… durch Maßnahmen entsprechend abgesichert ist

SERVICE REPORTING

Prüfung ausgewählter Kontrollen beim Dienstleistungsnehmer für ganze Kunden-gruppen.

Transparenter Prüfbericht in Form eines:

- ISAE 3XXX
- SOC1/SOC2
- IDW PS 951
- BSI C5
- …

© Ebner Stolz

Das Ganze mal umdrehen – Über die GoBD zum (Tax Compliance) MS

GRUNDSÄTZE ZUR ORDNUNGSMÄßIGEN FÜHRUNG UND AUFBEWAHRUNG VON BÜCHERN, AUFZEICHNUNGEN UND UNTERLAGEN IN ELEKTRONISCHER FORM SOWIE ZUM DATENZUGRIFF (GOBD)

GOBD VERFAHRENSDOKUMENTATION

Aufbewahrungs-pflichten	Archiv- & Dokumenten-management-systeme	Identifizierung steuerrelevanter IT-Systeme
IT-Tools & Technologien	Berechtigungs-konzepte	
Datenzugriff Finanzverwaltung	Aufzeichnungs-pflichten	**Identifizierung & Beschreibung IT-Kontrollen**

AUFBAU EINES TAX COMPLIANCE MANAGEMENTSYSTEMS

- Anforderungen und Kontrollen der GoBD als ein Teilbereich
- Zur Erweiterung von Anforderungen aus Einzelsteuergesetzgebung

© Ebner Stolz

Das ganzheitliche Managementsystem

1. PROZESS

- einheitliches und strukturiertes Vorgehen ist definiert und implementiert
- Integration weiterer Compliancegebiete möglich

2. COMPLIANCEANFORDERUNGEN

- Sollmaßnahmenkatalog ist vorhanden
- individuelle (unternehmensspezifische) Anforderungen sind erstellt
- Überschneidungen zwischen Normen werden erkannt
  (“erstelle einmal, verwende oft”)

4. ABSICHERUNG

- Internes Kontrollsystem als Umsetzungsnachweis und als Mittel zur Überwachung ist implementiert und wird gelebt (Kontrollframeworks nutzen)
- Wiederverwenden von Kontrollen möglich

3. RISIKOMANAGEMENT

- einheitliches und strukturiertes Risikomanagement ist umgesetzt
- Integration von Risiken “außerhalb” des Managementsystems möglich

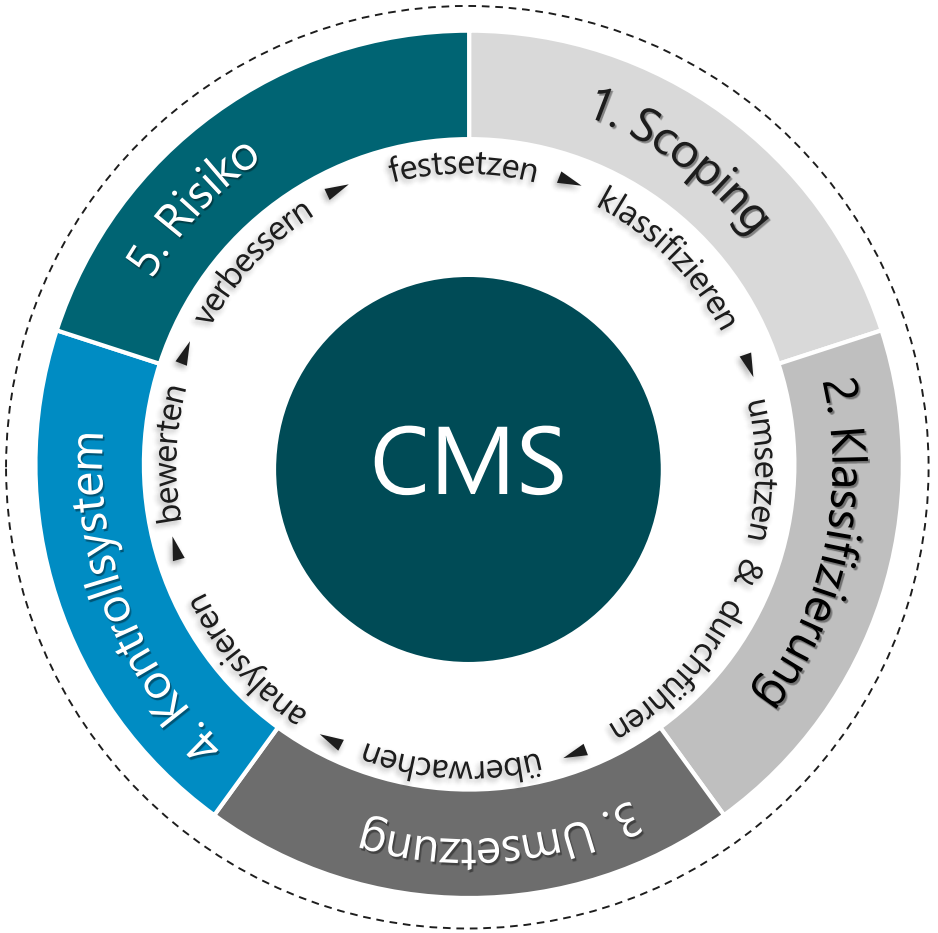
Und wie kann das nun konkret aussehen?

5. Risiko

- Gefährdungsmapping auf Risiken
- Ableiten Steuerungsentscheid und Maßnahmen
- **Risikoreduktion durch Kontrollen**

4. Kontrollsystem

- Durchführung von internen Kontrollen zur Sicherstellung der Wirksamkeit
- **Adressierung von Schwächen**



1. Scoping

- Festlegung des Anwendungs-bereiches sowie der Compliance-gebiete
- Definition der relevanten Geschäftsprozesse, Anwendungen, Infrastrukturkomponenten

2. Klassifizierung

- Festlegen der Objektrelevanz
- Schutzbedarfsfeststellung (SBF), Steuerrelevanz Persönlichkeitsrechtsverletzung (PRV)

3. Umsetzung

- Umsetzung der Compliance-anforderung
- Umsetzungsnachweis der Anforderung durch Dokumente
- **Nachweis der Umsetzung der Anforderung durch interne Kontrollen**
- **Umgang bei Nicht-Compliance (Erfassung von Gefährdungen)**

© Ebner Stolz

Ein Beispiel

Hintergrund:

- Quickfix der EU
- Neue Umsatzsteuervorschriften seit 1.1.2020 für den grenzüberschreitenden Handel (innergemeinschaftlicher Warenverkehr) nach der Änderung der Richtlinie 2006/112/EG zur Harmonisierung und Vereinfachung bestimmter Regeln des Umsatzsteuersystems

Beispiel einer Anforderung
(Anforderungsumsetzung)

Anforderung

Im Falle von innergemeinschaftlichem Warenverkehr ist sichergestellt, dass die Gültigkeit der Umsatzsteuer-ID-Nummer bei jeder Lieferung über die Internetseite des Bundeszentralamtes für Steuern geprüft wird. Die Prüfung ist nachvollziehbar zu dokumentieren.

Umsetzung

Automatischer Abruf der Gültigkeit durch das ERP-System und Speicherung des Datensatzes im ERP-System. In der Folge entweder automatische Sperrung der Transaktion bei ungültiger ID oder manuelle Entscheidung durch den Benutzer möglich.

IKS

Alternative K1: automatisch

Systemseitig wird die Bestellung verhindert, wenn keine gültige USt-ID vorliegt. Das Ergebnis wird dokumentiert.

Prüfungshandlung

Prüfen Sie ein Mal im Halbjahr die Systemeinstellungen.

Alternative K2: manuell

Es gibt eine Arbeitsanweisung, dass nur bei gültiger USt die Lieferung ausgelöst werden darf.

Prüfungshandlung

Prüfen Sie einmal pro Quartal, ob die formalen Vorgaben eingehalten und das Ergebnis dokumentiert wurde.

RKM

R1: bei Nichteinhaltung

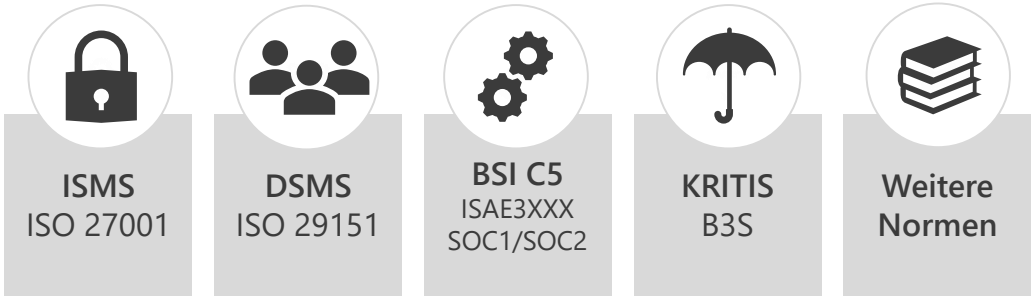
Es besteht das Risiko, dass eine steuerfreie innergemeinschaftliche Lieferung ohne Vorliegen der materiellen Voraussetzung der gültigen Umsatzsteuer bei der Lieferung angewandt wird. Das Unternehmen haftet in der Folge für die zu Unrecht nicht ausgewiesene USt.

Risikobehandlung

Einführung eines automatischen oder manuellen Prüfungsprozesses für die USt-ID.

© Ebner Stolz

Integrierter Managementsystemansatz



GANZHEITLICHER ANSATZ

Scoping / Schutzbedarfs-feststellung	Anforderungs-umsetzung	Interne Kontrollen	Risiko-behandlung
vernetzte Projektmethodik	Tool-Ansatz SGM	Anforderungs-mapping	Wiederver-wendbarkeit

ESecurity-CERT GmbH

Scoping / SBF

Projektentscheidend ist, die richtige Kombination von Normen für einen klar abgesteckten Anforderungsbereich festzulegen – **Konzentration auf das Geforderte**

Bewertung der Prozesse nur entsprechend ihrer Normenrelevanz (z. B. SBF, Grad der Persönlichkeitsrechtsverletzung) bewertet - **Konzentration auf das Wesentliche**

Umsetzung / IKS / RMS

Beginnen Sie gleich mit der Umsetzung der Anforderungen – **Keine umfassenden GAP-Analysen**

Etablieren Sie Kontrollen als ein Umsetzungsnachweis und leiten Sie steuerbare Risiken ab - **Machen Sie ihr Managementsystem lebbar**

Mapping / Wiederverwend-barkeit

Ähnliche Anforderungen aus unterschiedlichen Normenkreisen (z. B. ISO 27001 oder DSGVO) werden nur einmal, aber dafür ganzheitlich betrachtet.

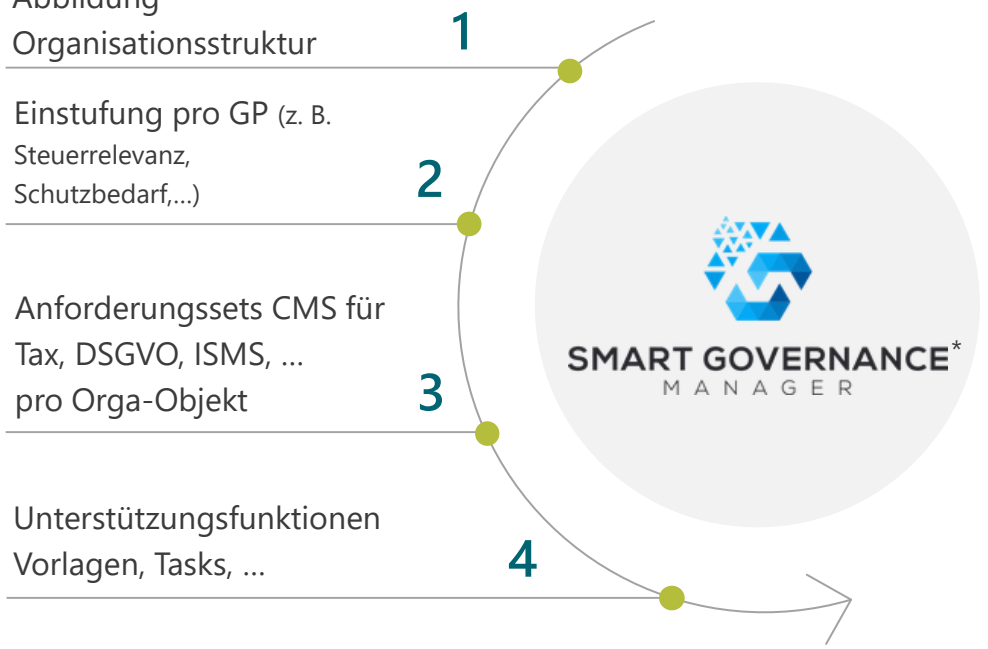
Richtlinien, interne Kontrollen und Maßnahmen zur Risiko-behandlung werden mehrfach als Umsetzungsnachweis verwertet – „**erstelle einmal, verwerte mehrfach**“

Aufbau eines ganzheitlichen Managementsystems

- Maßgeschneiderter und toolgestützter Projektansatz
- Remote- oder Vor-Ort/Coaching- oder Milestone Ansatz
- So detailliert wie notwendig, so praxisorientiert wie möglich

© Ebner Stolz

Tool-Ansatz – Aufbau eines Compliance Managementsystems (CMS) am Beispiel SGM



IKS

Nachweis der Erfüllung und kontinuierlichen Verbesserung der Anforderungen durch ein strukturiertes Internes Kontrollsystem (IKS).

RMS

Ableitung von Risiken auf Basis identifizierter Gefährdungen im Rahmen der Anforderungsumsetzung. Abbildung der Brutto-/ Nettorisikobewertung unter Berücksichtigung möglicher Risikobehandlungspläne.

CMS

Nachweis der Anforderungserfüllung für verschiedene Normenbereiche ohne Doppelarbeiten durch automatische Verknüpfungen der Orga-Objekte, Anforderungen, Risiken bei Nichterfüllung und interner Kontrollen als Einhaltungsnachweis.

* Gerne können wir Ihnen das Tool in einem separaten Termin kurz vorstellen.

© Ebner Stolz

Überblick – Optimierung durch Tool-Unterstützung (Beispiel Smart Governance Manager – SGM)

1 Scope

Wer bin ich?
- Organisatorischer Scope

Wer macht was?
- User und Rolle

2 Vorabbewertung

Wie wichtig ist der Prozess?
- SBF, PRV, TR, ...

Wie wichtig ist die Infrastruktur?
- Konfliktmanager

3 Anforderungs-erfüllung

Was muss ich machen?
- Meine Anforderungen

Erfülle ich es bereits?
- Erfüllungsgrad

Wie erfülle ich es?
- Norm, Vorlage, Kontext, ...

Wie belege ich es?
- Kontrollen
- Nachweise

Wie erheblich ist Nichterfüllung?
- Gefährdungen

4 Internes Kontrollsystem

Wer kontrolliert wann was?
- Kontrollmanagement

Was war Ergebnis der Kontrolldurchführung?
- Meine Kontrollen

Ich habe Schwächen festgestellt, was nun?
- Quicktask / Rückmeldung an Objekt-verantwortlichen

5 Risiko-management

Welche Gefährdung gehört zu welchem Risiko?
- Risikomapping

Wie hoch ist das Risiko?
- Meine Risiken

Was mache ich gegen das Risiko?
- Maßnahmen
- Kontrollen

6 Maßnahmen

Wer setzt wann was um?
- Maßnahmenmanagement

Wie ist der Umsetzungsstand?
- Meine Maßnahmen

Wird das Risiko gesenkt?
- Mein Risiko

Wird die Gefährdung gesenkt?
- Meine Anforderungen

7 Reifegrad

Wie umfassend sind die Anforderungen erfüllt?
- Reifegrad
- Meine Anforderungen

8 Definition der Metriken

Wie messe ich die Wirksamkeit meiner Umsetzung?
- KPI Management/Mapping
- Meine Anforderungen

die Farbe zeigt den Weg ins entsprechende SGM-Modul; siehe Nummern

© Ebner Stolz

Gliederung

Inhaltsverzeichnis

1 Ausgewählte Compliancenormen - Kurzvorstellung und aktuelle Entwicklung 3

2 Viele Anforderungen - Ein Ziel 26

3 Das Managementsystem - Potenziale erkennen und Bereiche mehrfach nutzen 34

4 Fragen 37

© Ebner Stolz

ANSPRECHPARTNER

Ihr Ansprechpartner

Mark Alexander Butzke

WP – StB – CISA – CRISC – CDPSE
ISO / IEC 27001 Senior Lead Auditor
Partner

mark.butzke@ebnerstolz.de
Tel. +49 89 549018-292
Mobil +49 179 4964724

Tätigkeitsschwerpunkte

- Handels- und steuerrechtliche IT Compliance
- Ganzheitliche integrierte Managementsysteme (ISMS, DSMS, CMS, TAX), u. a. nach ISO 27001, ISO 29151, KRITIS/B3S, BAIT, KAIT, TISAX, DSGVO, GoBD
- Begleitung von Datenschutz-projekten und -audits
- Business Continuity Management-systeme nach ISO 22301, BSI 100-4
- Interne Kontroll- und Risikomanagementsysteme
- Prüfung ausgelagerter Dienst-leistungen nach ISAE 3402/ISAE 3000 /IDW PS 951/SSAE 18/BSI C5
- ERP Projektbegleitung
- Prüfung revisions- und beweissicherer Lösungen zur elektronischen Dokumentenarchivierung und elektronischer Kassensysteme
- Aufbau von Verfahrens-dokumentationen

Branchenexpertise

- IT-Dienstleister
- Industrie und Handel
- Ernährung
- Transportwesen
- Finanzdienstleister
- Gesundheitswesen

© Ebner Stolz

Ihre Ansprechpartnerin

Sabine Riederer

Zertifizierte Datenschutzbeauftragte (GDD)
CDPSE – ISO 27001 Lead Auditor
Senior Managerin

sabine.riederer@ebnerstolz.de
Tel. +49 89 549018-271
Mobil +49 172 6892391

Tätigkeitsschwerpunkte

- Ganzheitliche integrierte Managementsysteme (ISMS, DSMS, CMS, TAX) u.a. nach ISO 27001, ISO 29151, KRITIS / B3S, BAIT, KAIT, TISAX, DSGVO, GoBD
- Ganzheitliche integrierte Managementsysteme
- Interne Kontroll- und Risikomanagementsysteme
- Aufbau und Implementierung von DSMS auf Basis der DSGVO
- Durchführung von Daten-schutzaudits, Aufbau der Datenschutzkonzeption und der Datenschutzorganisation
- Business Continuity Management-systeme nach ISO 22301, BSI 100-4

Branchenexpertise

- Automotive
- Produzierende Industrie
- Gemeinnützigkeit
- Kapitalmarktorientierte Unternehmen
- Banken