2. AUSGABE 2021

EBNER STOLZ

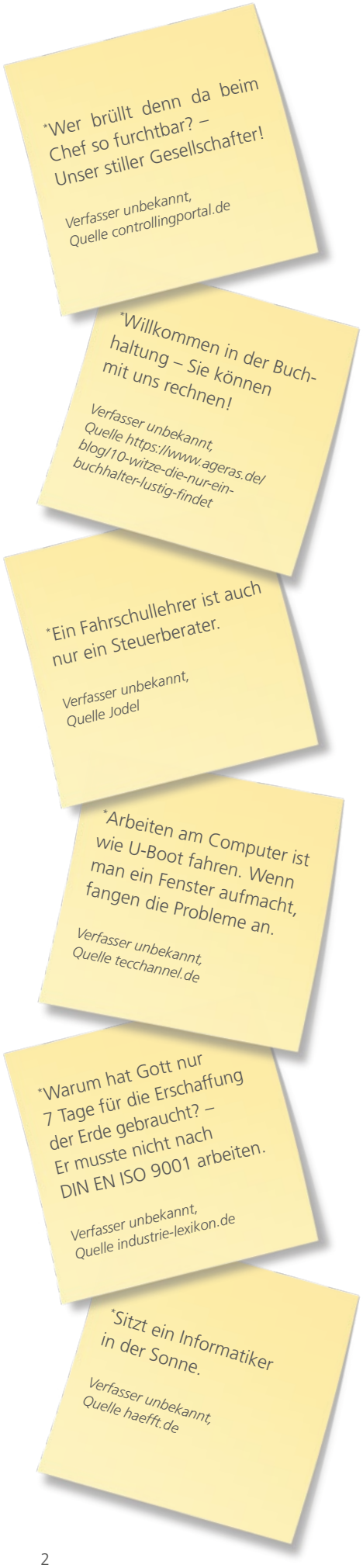
novus

INFORMATIONSTECHNOLOGIE

Das Informationsrisiko-management als IT-spezifische Anforderung der Finanz-aufsicht – wo liegen die Herausforderungen bei der Umsetzung in der Praxis?

Update von der „Kassen-Front“: EU-Taxameter im Fokus

KritisV 2.0 – Die große Erweiterung der Kritischen Infrastrukturen



„POST COVID ist ANTE COVID“, „COBIT statt COVID“ – „Prozessuale Neuorientierung?“

… kein Ende in Sicht

Dies sind die letzten beiden zentralen Überschriften, mit denen wir Sie als Leser in den letzten beiden IT-novi begrüßt haben. Ohne an dieser Stelle weiter auf das leider wieder aktuellere, allgegenwärtige Thema einzugehen, soll doch unsere zentrale Aussage bzw. unser Credo sein (explizite Empfehlung zur Nachahmung):

Wir lassen uns die Freude nicht nehmen!*

Pünktlich zum Jahresende freuen wir uns, Sie in unserem **neuen novus** zur **Informationstechnologie** über aktuelle Themen aus den Bereichen „IT & Wirtschaftsprüfung“, „IT-Recht“ und „IT-Sicherheit“ informieren zu können.

Nachdem wir Sie in den letzten Jahren immer rund um das Thema „IT-Sicherheitsgesetz“ informiert haben, gibt es nach Veröffentlichung der Version 2.0 ebenso eine Anpassung der Kritis-Verordnung. Also jener Verordnung, anhand derer definiert wird, welche Unternehmen als kritische Infrastruktur (Kritis) einzustufen sind. Die Herabsetzung zentraler Schwellwerte führt dazu, dass eine dreistellige Anzahl an Unternehmen die entsprechenden Anforderungen erfüllen müssen – und dies gegenwärtig ohne bekannte Umsetzungsfrist. Daher stellt der Artikel auch einen Schwerpunkt in diesem novus dar.

Ein weiterer Schwerpunkt richtet sich auf das Informationsrisikomanagement im Bereich der Finanzaufsicht und deren Praxisumsetzung.

Die GoBD sind (wieder) in aller Munde. Über einen neuen IDW Prüfungshinweis sowie mögliche Konsequenzen bei Mängeln in der Umsetzung von GoBD-Vorgaben wollen wir Sie informieren. Zudem stellen wir Ihnen gerne die Neuerungen von der „Kassen-Front“ im Sinne von Änderungen der Kassensicherungsverordnung vor.

Wir wünschen Ihnen, Ihren Familien und Angehörigen ein frohes und gesegnetes Weihnachtsfest verbunden mit Glück, Freude und Erfolg. Lassen Sie uns gemeinsam gesund und gestärkt in 2022 gehen.

Ihr GBIT

ESecurity-CERT GmbH – Akkreditiert für den IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG

Nachdem die ESecurity-CERT GmbH im Jahr 2020 erfolgreich den Akkreditierungsprozess der Deutschen Akkreditierungsstelle GmbH (DAkkS) für die Zertifizierung von Management-Systemen nach der internationalen Norm DIN EN ISO/IEC 27001:2017-06 durchlaufen hat, wurde nun ebenfalls der Akkreditierungsprozess zur Durchführung von Audits nach dem IT-Sicherheitskatalog gemäß § 11 Abs. 1a Energiewirtschaftsgesetz (EnWG) erfolgreich abgeschlossen.Somit hat die ESecurity-CERT offiziell die Möglichkeit, auch die eingerichteten Management-Systeme aller Strom- und Gasnetzbetreiber, welche nach der KRITIS-Verordnung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-KRITISV) unter den festgelegten Schwellwerten fallen, zu zertifizieren.

IT-Sicherheitskatalog 1a

Am 12.08.2015 veröffentlichte die Bundesnetzagentur den IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG für Netzbetreiber. Dieser IT-Sicherheitskatalog bezweckt die Sicherstellung eines angemessenen Schutzes gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind. Der IT-Sicherheitskatalog stellt spezifische Anforderungen in Bezug auf die Informationssicherheit. Netzbetreiber (wie z. B. Stadtwerke), welche die Schwellenwerte der BSI-KritisV erreichen bzw. überschreiten, sind verpflichtet, die Anforderungen dieses Sicherheitskatalogs umzusetzen. Mit einer Zertifizierung weist die geprüfte Organisation den Stand und die Qualität des eingerichteten Informationssicherheitsmanagements (ISMS) durch eine unabhängige Prüfung nach.

Auditierung des IT-Sicherheitskatalogs 1a

Die Auditierung nach dem IT-Sicherheitskatalog 1a erfolgt analog einer Zertifizierungsprüfung nach DIN EN ISO/IEC 27001: 2017-06.

Exkurs Akkreditierung

Jede Zertifizierungsstelle muss zur Durchführung von Zertifizierungsaudits nach definierten Standards bzw. Normen einen mehrmonatigen Akkreditierungsprozess durchlaufen. Zu diesen Normen gehören neben der ISO/IEC 27001 sowie dem IT-Sicherheitskatalog gemäß EnWG auf der Grundlage der ISO/IEC 27006 bspw.:

- Umweltmanagement-Systeme auf der Grundlage der DIN EN ISO 14001:2015
- Energiemanagement-Systeme auf der Grundlage der DIN EN ISO 50001:2018
- Management-Systeme zur Korruptionsbekämpfung nach DIN ISO 37001
- Compliance-Management-Systeme – Anforderungen mit Anleitung zur Anwendung gemäß ISO 37301.

AUDITPLANUNG
(organisatorische Abstimmung)

Festlegung

- Geltungsbereiche (Geschäftstätigkeit und/oder Standorte
- Termine
- Interviewpartner
- Prüfbereiche:
  - Abteilungen
  - Räumlichkeiten

ZERTIFIZIERUNGSAUDIT
(Umfang abhängig von Größe und Komplexität der Organisation)

Stage 1: Dokumentationsprüfung des ISMS ← **KORREKTUR!**

- Grundlegende Beurteilung und Würdigung des Geltungsbereiches sowie der grundsätzlichen Anforderungserfüllung
- Ermittlung der grundlegenden Prüfungsbereitschaft im Hinblick auf die Stage 2-Prüfung, ggf. Aufzeigen von Handlungsbedarf, Ableitung des individuellen Auditplans für die Stage 2-Prüfung
- Bewertung der Dokumentation — **ABWEICHUNG?**

Stage 2: Prüfung Wirksamkeit ISMS ← **KORREKTUR!**

- Feststellung der Konformität des Management-Systems mit den Auditkriterien
- Beurteilung der Fähigkeit des Management-Systems, die Erfüllung der geltenden gesetzlichen, behördlichen und vertraglichen Anforderungen sicherzustellen
- Beurteilung der Wirksamkeit des Management-Systems in Bezug auf die Sicherstellung, dass die Kundenorganisation dauerhaft ihre festgelegten Ziele erfüllt

Auditorentätigkeit

- Beobachten
- Nachweisen
- Aufzeichnen
- Schussfolgern
- Berichten

ABWEICHUNG?

Das Informationsrisikomanagement als IT-spezifische Anforderung der Finanzaufsicht – wo liegen die Herausforderungen bei der Umsetzung in der Praxis?

Vorwort

Spätestens seit der Veröffentlichung der bankaufsichtlichen Anforderungen an die IT im November 2017 ist der Umgang mit Risiken aus der Informationstechnologie ein wesentlicher Bestandteil des Risikomanagements eines jeden Instituts. Hierbei ergibt sich die steigende Relevanz für das Management IT-spezifischer Risiken nicht nur aus den regulatorischen Anforderungen, sondern auch aus einer gestiegenen Bedrohungslage für die IT der Unternehmen sowie einer zunehmenden Digitalisierung von Geschäftsmodellen und -prozessen. Wie die Praxis der letzten Jahre jedoch gezeigt hat, stellt die konkrete Ausgestaltung eines angemessenen und gleichzeitig praktikablen Informationsrisikomanagements die meisten Institute vor erhebliche Herausforderungen. Oftmals beginnt die Schwierigkeit im Rahmen der Umsetzung bereits bei einem einheitlichen Verständnis des Risikobegriffs und setzt sich über die Auswahl eines geeigneten Risikomanagementprozessmodells, der aufbau- und ablauforganisatorischen Ausgestaltung sowie der Integration in das Gesamtrisikomanagement des Instituts fort. Wir möchten ein grundsätzliches Verständnis für die Systematik eines ganzheitlichen Informationsrisikomanagement-Systems vermitteln. Zudem zeigen wir wesentliche Herausforderungen und Lösungsansätze aus der Praxis auf.

Einordnung der regulatorischen Anforderungen in Bezug auf IT-spezifische Risiken

Zur Gewährleistung einer ordnungsgemäßen Geschäftsorganisation muss ein Institut nach § 25a KWG bzw. AT 2.2 und AT 4 MaRisk über ein angemessenes und wirksames Risikomanagement verfügen. Das Risikomanagement dient insb. als Grundlage für eine laufende Beurteilung und Sicherstellung der Risikotragfähigkeit des Institutes. Hierbei sind mindestens die folgenden, aus Sicht der Aufsicht wesentlichen Risiken zu berücksichtigen:

- Adressenausfallrisiken (einschließlich Länderrisiken),
- Marktpreisrisiken,
- Liquiditätsrisiken und
- operationelle Risiken.

Die bankaufsichtlichen Anforderungen an die IT (BAIT) beinhalten in Bezug auf das Risikomanagement des Institutes spezifische Anforderungen zum Management von drei Risikounterarten des operationellen Risikos. Dies sind die

- Informationsrisiken (IT-Risiken),
- IT-Projektrisiken sowie
- Risiken aus dem sonstigen Fremdbezug von IT-Dienstleistungen bzw. (wesentlichen) Auslagerungen.

Im Fokus dieses Artikels stehen die Informationsrisiken. Es ist aus unserer Sicht unbedingt anzuraten, eine Betrachtung der anderen beiden Risikounterarten im Rahmen der Ausgestaltung der eigenen Risikotaxonomie der operationellen Risiken vorzunehmen.

Begriffsverständnis Informationsrisiken

nachzuvollziehen, wie eine Abgrenzung zwischen Informationsrisiken (oder auch Informationssicherheitsrisiken genannt) und IT-Risiken erfolgt. Informationsrisiken und IT-Risiken haben zwar eine große Schnittmenge, können aber nicht ohne Weiteres einfach gleichgesetzt werden. So betrachten Informationsrisiken auch Risiken für Nicht-IT-Werte (wie bspw. Papierakten), die keine IT-Risiken darstellen. Zugleich kann es IT-Risiken geben, bei denen der zu schützende Wert keine Information darstellt (wie bspw. der Inhalt eines Bargeldautomaten). In der Praxis gibt es hierzu unterschiedliche Ansätze, wobei eine Integration der IT-Risiken in die Risikounterart Informationsrisiko die gängigste Vorgehensweise ist. Dies betrifft ebenso spezifische IT-Risiken, wie bspw. die Cyber-Risiken. Die Aufsicht hat eine entsprechende Denkweise und ersetzte in den vergangenen Jahren den Begriff IT-Risiko sukzessive in ihren Rundschreiben durch das Informationsrisiko. Wie auch immer die Risikotaxonomie ausgestaltet ist, es muss immer sichergestellt sein, dass alle relevanten Risiken in das Risikomanagement des Instituts mit einbezogen sind.

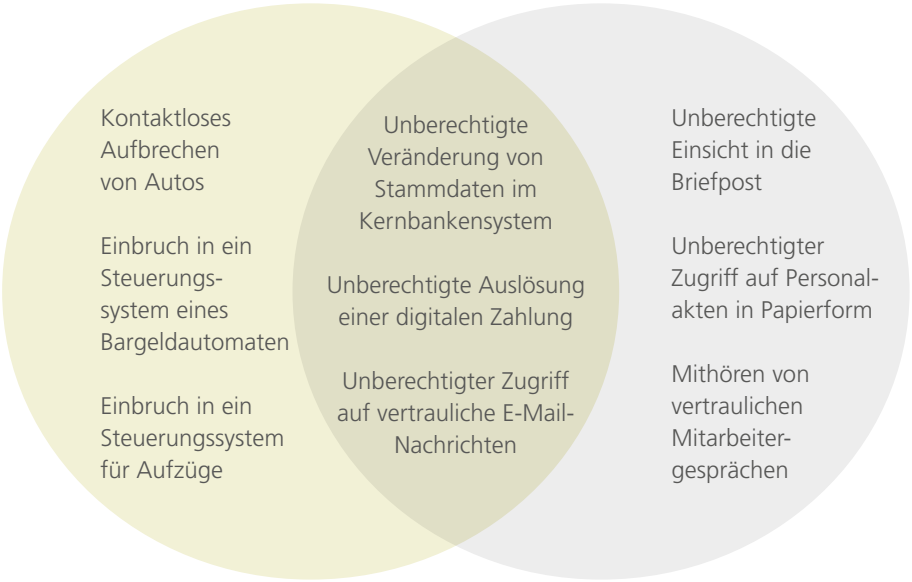


Schaubild: Abgrenzung Informationsrisiko/IT-Risiko

Auswahl und Ausgestaltung des Informationsrisikomanagement-Systems

Grundsätzlich verfolgen alle Risikomanagement-Systeme das Ziel, Risiken zu identifizieren, zu bewerten und zu steuern bzw. zu überwachen. Dies gilt ebenfalls für das Informationsrisikomanagement. Nun gibt es natürlich auch hier unterschiedliche Ansätze für die Ausgestaltung der einzelnen Prozessschritte. Ratsam ist es, sich hierbei an gängigen Standards zu orientieren. Dies ist auch seitens der Aufsicht unbedingt gefordert. Die zwei bekanntesten Standards für die Umsetzung eines Informationsrisikomanagement-Systems sind die ISO-Norm 27005, als verbindende Norm zwischen der ISO 27001 und der ISO 31000, sowie der BSI-Standard 200-3. Beide Standards verfolgen eine ähnliche Herangehensweise, wobei sie sich im Detail durchaus unterscheiden. Die ISO-Norm 27005 ist insgesamt generischer vom Ansatz und bietet daher dem Unternehmen die Möglichkeit einer individuelleren Umsetzung. Der Ansatz des BSI-Standard 200-3 bietet konkretere Hilfestellungen für die Implementierung, kann aber – wie häufig in der Praxis beobachtet – dazu verleiten, die individuelle Risikosicht des Instituts zu vernachlässigen. Welcher Standard auch herangezogen wird, er sollte immer mit den regulatorischen Anforderungen sowie dem Rahmenwerk des Informationssicherheitsmanagements (z. B. der ISO-Norm 27001) in Einklang stehen und diesbezüglich regelmäßig überprüft und ggf. angepasst werden.

Die erste Herausforderung im Rahmen der Implementierung der einzelnen Prozessschritte des Informationsrisikomanagements betrifft die Identifizierung von Informationsrisiken. Hier gilt es zuerst einmal zu verstehen, über welche Systematik bzw. welchen Kanal Informationsrisiken auf der Grundlage der gängigen Vorgehensmodelle identifiziert werden. Als gängiges Vorgehensmodell ist insb. der „Checklisten-Ansatz" zu nennen, der auch in den BAIT im Kapitel zum Informationsrisikomanagement beschrieben wird. Der Ansatz basiert auf einer Erhebung aller Informationskomponenten (Infrastrukturanalyse) und dem daraus erstellten Informationsverbund. Der Informationsverbund kann hierbei unterschiedlich detailreich ausgestaltet werden. Im Wesentlichen sind hierin jedoch für das Geschäft relevante Informationen als oberste Ebene des Informationsverbundes, Prozesse sowie Teilprozesse – in denen die Informationen als In- und Output-Faktoren verarbeitet werden – sowie für die Prozesse und Teilprozesse relevante Anwendungssysteme, Datenbanken, Server, Netzwerkkomponenten und Gebäude einzubeziehen. Die einzelnen Informationskomponenten sind im Hinblick auf ihre gegenseitige Abhängigkeit bei der Informationsverarbeitung miteinander zu verknüpfen. Diese Verknüpfung der einzelnen Informationskomponenten ist die Grundvoraussetzung für die spätere Vererbung der Schutzbedarfe im Rahmen der Schutzbedarfsfeststellung. Daher ist es auch von so großer Bedeutung, dass die Vollständigkeit der Informationskomponenten (inklusive deren bestehende Abhängigkeiten) sichergestellt ist. Oftmals besteht in der Praxis die Schwierigkeit, dass keine vollständige Landkarte der Geschäftsprozesse vorliegt, was zu einem erheblichen Aufwand führen kann, wenn diese erst erstellt werden muss. Zugleich zeigt dies bereits beim Aufbau eines Informationsrisikomanagementprozesses, dass das Management von Informationsrisiken eine unternehmensweite und durchaus komplexe Aufgabe ist. Neben den bereits genannten Informationskomponenten ist dringend anzuraten, auch durch die Fachbereiche betriebene oder entwickelte Anwendungen (sog. individuelle Datenverarbeitungen) sowie Dienstleister in den Informationsverbund mit aufzunehmen. Durch die Aufnahme von Dienstleistern wird auch den weiteren Konkretisierungen der Anforderungen der BAIT vom 16.08.2021 nachgekommen, in denen die Vernetzung des Informationsverbundes mit Dritten explizit gefordert ist. Alle Informationskomponenten sind zu inventarisieren und deren Aktualität ist anhand von Kontroll- und Überwachungsmaßnahmen durchgehend sicherzustellen. Als Inventar bietet sich eine Bestandsverwaltung in Form einer Configuration Management Database (kurz CMDB) an.

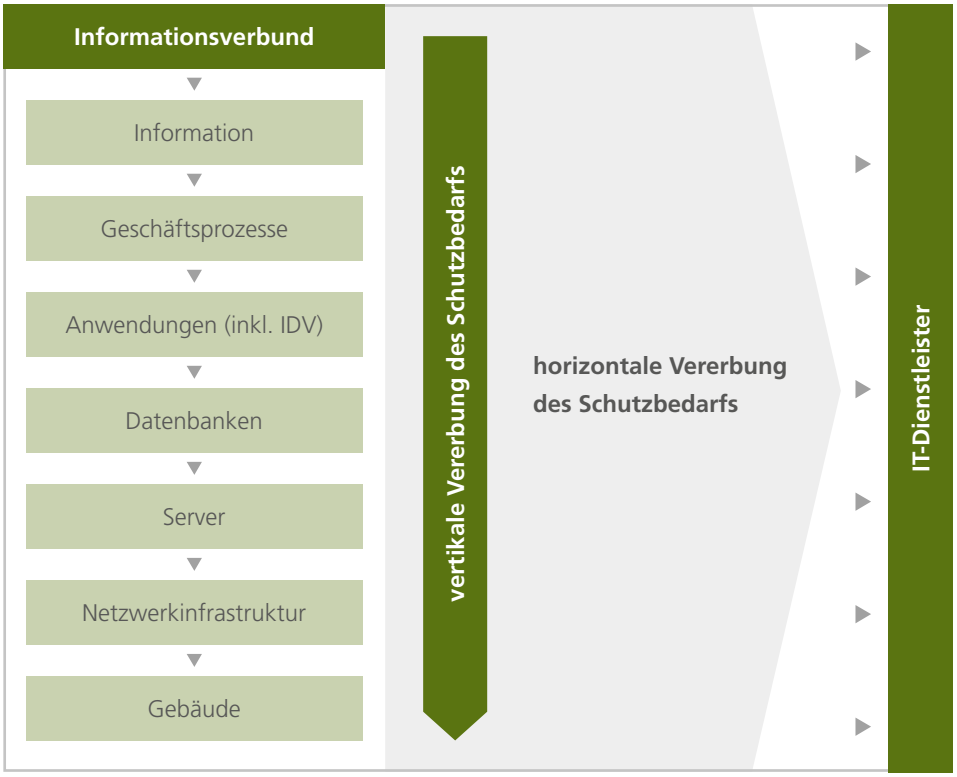


Schaubild: Informationsverbund

Ist ein vollständiger Informationsverbund geschaffen, gilt es, den Schutzbedarf für die einzelnen Informationskomponenten zu bestimmen und mindestens jährlich bzw anlassbezogen zu aktualisieren. Hierbei sind mindestens die vier Schutzziele

- Vertraulichkeit,
- Integrität,
- Verfügbarkeit und
- Authentizität

zu bewerten.

Hinweis: Die Authentizität wird häufig auch als Teil der Integrität definiert.

Die Schutzbedarfsfeststellung erfolgt in der Praxis häufig noch auf Anwendungsebene. Dies ist nicht zielführend und aus Sicht der Aufsicht auch nicht angemessen, da es bei der Schutzbedarfsfeststellung im Wesentlichen darum geht, das angestrebte Schutzniveau der Informationen zu bestimmen und davon abhängig, das Schutzniveau aller Informationskomponenten, die bei der Verarbeitung der jeweiligen Information eingebunden sind. Zielführender ist, die Schutzbedarfsfeststellungen auf der Geschäftsprozessebene unter Einbezug der hierbei verarbeiteten Informationen durchzuführen. Im Anschluss sind die ermittelten Schutzbedarfe mit geeigneten Verfahren auf die einzelnen im Geschäftsprozess verwendeten IT-Komponenten zu vererben. Die erfolgten Schutzbedarfsanalysen sowie die hierzu angefertigte Dokumentation ist gemäß den weiteren Konkretisierungen der Anforderungen der BAIT vom 16.08.2021 im Anschluss durch das Informationsrisikomanagement zu überprüfen.

Für die ermittelten Schutzniveaus der Informationskomponenten gilt es, nun Schutzmaßnahmen in Form eines Sollschutzmaßnahmenkataloges zu definieren. Hierbei kann auf bestehende Anforderungskataloge, wie z. B. auf die ISO-Norm 27001 (Annex A) oder auf das IT-Grundschutzkompendium des BSI, zurückgegriffen werden. Hierbei ist jedoch ausdrücklich darauf hinzuweisen, dass individuelle Anforderungen, die sich bspw. aus dem Geschäftsmodell oder der institutseigenen Gefährdungslage ergeben, mit einbezogen werden sollten. Zudem sind auch spezifische externe Anforderungen wie u. a. die der Aufsicht (wie die MaRisk, BAIT, EBA GL), die des Bundesministeriums für Finanzen (wie die GoBD) oder die von Instituten, die unter den § 8a BSIG (Kritis) fallen, zu berücksichtigen.

Im nächsten Schritt gilt es nun, auf der Basis der Anforderungskataloge, die bspw. aus der ISO/IEC 27001 abgeleitet sein können, Schwachstellen zu identifizieren. Hierzu werden Soll-Ist-Abgleiche durchgeführt, anhand derer konkret festgestellt wird, inwiefern die Sollschutzmaßnahmen in Form von Ist-Schutzmaßnahmen im Institut umgesetzt wurden. Ein entsprechender Abgleich kann im Rahmen eines risikoorientierten Auditplans oder auch im Rahmen eines den Soll-Maßnahmen zu geschlüsselten internen Kontrollsystems erfolgen. Die ermittelten Schwachstellen sind der erste Hinweis auf ein mögliches Risiko.

An dieser Stelle stellt sich die Frage, ob ausschließlich über dieses Vorgehen und die hieraus festgestellten Schwachstellen Informationsrisiken identifiziert werden können bzw. sollten. Die Antwort lautet ganz klar nein. Es gibt viele weitere Wege, über die Schwachstellen und damit potentielle Informationsrisiken zu erkennen sind. Dies sind bspw. Ad-hoc-Meldungen aus den Fachabteilungen, Major-Incidents, Feststellungen aus Prüfungsberichten oder Berichten aus Sicherheitsanalysen, wie einem Penetrationstest, festgestellte Abweichungen aus dem Notfallmanagement und der Dienstleisterüberwachung. Die Liste könnte beliebig weitergeführt werden. Daher sollte jedes Institut im Zuge des Aufbaus seines eigenen Informationsrisikomanagementsystems individuell eruieren, welche Wege hier zu betrachten sind.

Mit den identifizierten Schwachstellen geht es nun in den Prozess der Risikoanalyse. Hierbei ist es wichtig zu verstehen, dass Schwachstellen nicht per se eine Gefährdung, bzw. dieser nachgelagert, ein Informationsrisiko darstellen. Hierzu müssen noch eine relevante Bedrohung sowie ein Informationswert, der durch die Schwachstelle und die Bedrohung einer Gefährdung unterliegt, hinzukommen. Bedrohungen werden in der Praxis häufig auf der Grundlage von standardisierten Bedrohungskatalogen (z. B. vom BSI) für die Risikoanalyse herangezogen. Um die spezifische Bedrohungslage des eigenen Instituts aber wirklich beurteilen zu können und zu kennen, ist es dringend geboten, regelmäßig auch eigenständig Bedrohungsanalysen durchzuführen. Dies ist ebenfalls aus Sicht der Aufsicht erforderlich. Wurden relevante Gefährdungen festgestellt, geht es im Prozessverlauf weiter zur Bewertung des Informationsrisikos.

Hinweis: Risiken sind gemäß Definition des BSI relevante und bewertete Gefährdungen.

Im Rahmen der Risikobewertung wird der Risikowert (Erwartungswert) anhand des Schadenpotentials, also dem möglichen Schadenswert des Schadensereignisses, sowie der Schadenshäufigkeit, also der Wahrscheinlichkeit des Schadensereignisses, berechnet. Hierzu wird oftmals eine Risikomatrix herangezogen, die zugleich Risikoklassen unter Einbezug des Risikoappetits des Instituts beinhaltet. Die Parameter der Risikobewertung innerhalb des Informationsrisikomanagements müssen immer die Werte/Methodik des Risikomanagements des Instituts wiedergeben. Dabei ist wichtig zu berücksichtigen, dass das Informationsrisikomanagement Teil des Gesamtrisikomanagements des Instituts ist und somit nicht anderen Regeln folgen kann. Die Risikobetrachtung kann hierbei in Form von Brutto- und Netto-Risiken erfolgen. Alle Risiken sind in einem Risikoinventar zu erfassen.

Die identifizierten und bewerteten Informationsrisiken müssen im nächsten Schritt, wie alle Risiken des Instituts, gesteuert und überwacht werden. Auch hier gilt es, die Methodik und Vorgaben des Risikomanagements des Instituts zu übernehmen. Dies können bspw. Regelungen zur Höhe und Genehmigung von Risikoakzeptanzen sein. Grundsätzlich stehen klassisch folgende Steuerungsoptionen für die Informationsrisiken zur Auswahl:

- Risikovermeidung (z. B. Workarounds),
- Risikotransfer (z. B. IT-Versicherungen),
- Risikominderung (z. B. zusätzliche Schutzmaßnahmen oder Kontrollen) und
- Risikoakzeptanz (z. B. Akzeptanz von geringeren Risiken durch das Management).

Wie die Steuerungsprozesse schlussendlich ausgestaltet werden, ist abhängig vom jeweiligen Risikomanagement des Instituts und kann daher in der Praxis sehr unterschiedlich sein. Gleiches gilt für die Synchronisierung des vorgelagerten Informationsrisikomanagements mit dem Management der

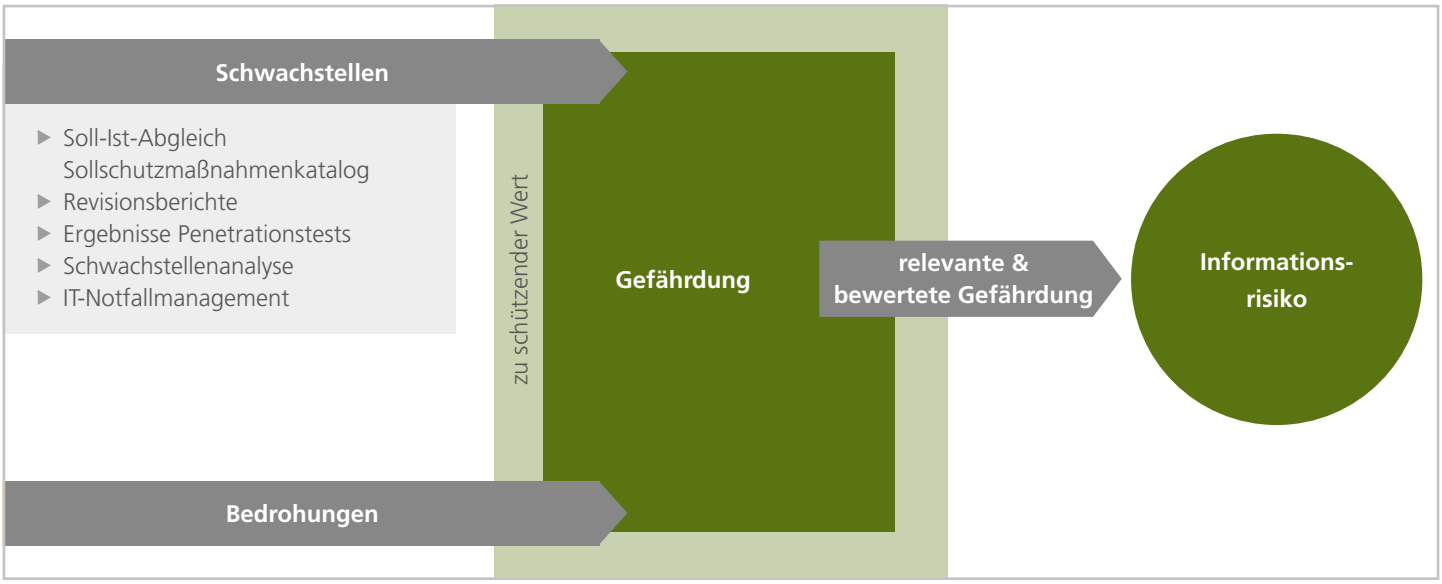


Schaubild: Identifikation von Risiken

operationellen Risiken. Da Informationsrisiken Bestandteil der operationellen Risiken sind, müssen auch diese im Rahmen der Risikotragfähigkeitsberechnung des Instituts berücksichtigt werden. Hier gibt es in der Praxis unterschiedliche Ansätze, wie und ab welcher Höhe die Informationsrisiken hier mit einbezogen werden sowie in welcher Form die Meldung der Informationsrisiken an das Risikocontrolling erfolgt. Wichtig ist hierbei, dass die Prozesse den Vorgaben des Risikomanagements des Instituts stringent folgen und dass alle Risiken auf der Ebene des Informationsrisikomanagements oder des Risikocontrollings effektiv gesteuert werden.

Damit das Informationsrisikomanagement seinen Aufgaben wirksam und zielführend nachkommt, ist es ebenfalls wichtig, dass eine regelmäßige Evaluierung der Prozesse des Informationsrisikomanagement-Systems vorgenommen wird. Das Thema der kontinuierlichen Verbesserung wird derzeit in der Praxis noch stark vernachlässigt. Hier sollten entsprechende interne Kontrollsysteme aufgebaut sowie Management-Reviews in geregelten Abständen erfolgen. Hinweise auf die Effizienz des Informationsrisikomanagement-Systems kann hierbei auch die durch die in den BAIT geforderte Berichterstattung an die Geschäftsleitung geben, wenn diese entsprechend detailliert ausgestaltet ist.

Herausforderungen bei der aufbauorganisatorischen Ausgestaltung eines Informationsrisikomanagements

Abschließend soll an dieser Stelle noch einmal kurz auf die aufbauorganisatorische Ausgestaltung des Informationsrisikomanagements eingegangen werden, da dieses Thema in der Praxis in Teilen Diskussionsbedarfe hervorruft. Das Informationsrisikomanagement ist eine Aufgabe der zweiten Verteidigungslinie des Unternehmens. Somit darf die Funktion nicht durch den Bereich IT, als erste Verteidigungslinie, ausgeübt werden. Vielmehr muss die Funktion unbedingt vom Bereich IT unabhängig ausgestaltet sein. Üblicherweise wird das Informationsrisikomanagement durch das Informationssicherheitsmanagement – oftmals durch den Informationssicherheitsbeauftragten – durchgeführt bzw. von diesem verantwortet. Hintergrund hierfür ist, dass das Informationsrisikomanagement einen der wesentlichen Managementprozesse eines Informationssicherheitsmanagement-Systems darstellt (siehe z. B. die ISO-Norm 27001) und somit nur schwierig durch andere Funktionen, wie z. B. dem Risikocontrolling des Instituts, verantwortet werden kann. Weiterhin ist für die effektive Steuerung und Überwachung eines Informationsrisikomanagements spezifisches IT-Wissen erforderlich, worüber in der Regel nur das Informationssicherheitsmanagement und der Bereich IT im Institut verfügt. Neben der Verantwortung für die Überwachung und Steuerung des Informationsrisikomanagement-Systems gibt es noch weitere Aufgaben und Verantwortungsbereiche innerhalb der Prozesse des Managements von Informationsrisiken. Dies betrifft insb. die Verantwortung für die Bewertung und Steuerung von Einzelrisiken. Diese Verantwortung liegt immer bei dem jeweiligen Risikoeigentümer, der in den meisten Fällen der Eigentümer der durch die Auswirkung des Risikos betroffener Informationen bzw. des Geschäftsprozesses ist. Nur dieser Risikoeigentümer kann eine Entscheidung hinsichtlich Risikobewertung und Risikosteuerung treffen. Das Informationsrisikomanagement kann diese Entscheidung, wie zum Teil in der Praxis gesehen, nicht treffen. Eine beratende Funktion des Informationsrisikomanagements ist hier aber durchaus notwendig.

IDW Prüfungshinweis zur GoBD-Compliance

Im Rahmen von Jahresabschlussprüfungen ergeben sich immer häufiger Fragestellungen in Bezug auf die angemessene und wirksame Umsetzung der Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff, sog. GoBD-Anforderungen des BMF (Schreiben vom 28.11.2019). Diesen GoBD-Anforderungen kann im Rahmen der Jahresabschlussprüfung abschließend nur schwer Rechnung getragen werden. Auch die immer weiter vorangetriebene Digitalisierung, insb. im Bereich der Belegarchivierung, begründet die Notwendigkeit einer Konkretisierung zur Umsetzung von GoBD-Anforderungen im Einzelfall.

Der IDW Prüfungsstandard 860 (IDW PS 860) regelt die Grundsätze und Vorgehensweisen, wonach IT-Prüfungen außerhalb der Abschlussprüfung durchzuführen sind. Zur praktischen Umsetzung des IDW PS 860 veröffentlichte der Fachausschuss IT (FAIT) bereits Prüfungshinweise zu den Themen Datenschutz, kritische Infrastrukturen sowie Cloud-Dienste. Mit dem IDW PH 9.860.4 reagiert das IDW mit einem Prüfungshinweis zur Prüfung der GoBD-Compliance nun auch auf diesen Bedarf aus der Praxis.

Der am 14.07.2021 vom FAIT verabschiedete PH 9.860.4 konkretisiert, wie die GoBD-Anforderungen im Sinne der Darstellung geeigneter Kriterien zur Einrichtung angemessener Grundsätze, Verfahren und Maßnahmen des IT-Systems angemessen umgesetzt werden können.

Aus dem PH 9.860.4 ergibt sich ein modularer Aufbau der Prüfung der GoBD-Compliance. So ist grundsätzlich das sog. Basiselement Prüfungsgegenstand. Darüber hinaus ist zusätzlich mindestens eins der vier genannten Ergänzungselemente Bestandteil der Prüfung. Die Prüfung kann sowohl als reine Angemessenheitsprüfung aber auch zusätzlich als Wirksamkeitsprüfung durchgeführt werden.

Basiselement

Das Basiselement umfasst die Verfahrensdokumentation und generelle IT-Kontrollen. Da nach Auffassung der Finanzverwaltung eine aussagefähige, vollständige und aktuelle Verfahrensdokumentation Voraussetzung für die Nachvollziehbarkeit und Nachprüfbarkeit eines IT-gestützten Verfahrens ist, stellt diese die Basis einer jeden Prüfung der GoBD-Compliance dar. Zunächst werden im Rahmen des Basiselements die grundsätzlichen GoBD-Vorgaben zur Erstellung und Aktualisierung einer Verfahrensdokumentation betrachtet. Im Rahmen der Ergänzungselemente (s. u.) werden zudem die geschäftsprozessspezifischen Aspekte der Verfahrensdokumentation berücksichtigt.

Im Rahmen des Basiselements fokussiert sich die Prüfung der Angemessenheit (und Wirksamkeit) der generellen IT-Kontrollen auf Kontrollaktivitäten in den Bereichen

- Change Management (Programm- und Datenänderungsverfahren),
- Zugang und Zugriff auf IT-Systeme (Datensicherheit),
- Prozesse zum Betrieb der IT-Infrastruktur (IT-Betrieb).

Insb. anwendungsbezogene IT-Kontrollen sind – geschäftsprozessunabhängig – Bestandteil im jeweiligen Ergänzungselement.

Ergänzungselemente

Der Prüfungshinweis sieht vier Ergänzungselemente vor:

1. Belegeingang
2. Elektronischer Belegausgang
3. Elektronische Aufbewahrung
4. Datenzugriff der Finanzverwaltung.

Das Ergänzungselement Belegeingang betrachtet zunächst generelle GoBD-Vorgaben für den Belegeingang. Darauf aufbauend werden spezifische GoBD-Vorgaben für die bildliche Erfassung von eingehenden Papierbelegen, für den elektronischen Belegeingang sowie für die Rechnungseingangsprüfung berücksichtigt.

Im Modul Elektronischer Belegausgang wird hinsichtlich der sich unterscheidenden Anforderungen zwischen unstrukturierten Informationen (Bildformate) und strukturierten Informationen (Daten) differenziert. Die vorangestellten generellen Vorschriften sind grundsätzlich bei allen Prozessschritten zum Ausgang elektronischer Belege zu berücksichtigen.

Das Modul Elektronische Aufbewahrung umfasst die Prüfung von Maßnahmen zur Erfüllung der gesetzlichen Aufbewahrungspflichten. Beim Einsatz von Archivierungsverfahren muss über den gesamten Prozess der Archivierung sichergestellt sein, dass alle Dokumente und Daten gemäß dem Archivierungskonzept erfasst werden. Daneben muss sichergestellt werden, dass die Daten und Dokumente für die Dauer der Aufbewahrungspflicht (innerhalb einer angemessenen Zeit) wiedergegeben werden können.

Das Ergänzungsmodul Datenzugriff der Finanzverwaltung bezieht sich auf die Anforderungen zur Einsichtnahme in die gespeicherten Daten und/oder die Nutzung der IT-Systeme zur Prüfung dieser Unterlagen durch die Finanzverwaltung im Rahmen einer steuerlichen Außenprüfung bzw. Umsatzsteuer-Nachschau. Ebenfalls werden die Vorgaben zur maschinellen Auswertbarkeit berücksichtigt.

Mit diesem modularen Aufbau wird die Relevanz des IT-Kontrollsystems als integraler Bestandteil der GoBD-relevanten IT-Systeme unterstrichen. Die Beurteilung der Angemessenheit und Wirksamkeit eines Geschäftsprozesses ist ohne die Berücksichtigung des IT-Kontrollsystems nicht möglich. Hierdurch kommt denjenigen Grundsätzen, Verfahren und Maßnahmen des IT-Systems zur Bewältigung der Risiken aus dem Einsatz von IT (vgl. GoBD, Rn. 103 ff.) eine wesentliche Bedeutung zu.

Ebenso wird die Relevanz einer aussagefähigen, vollständigen und aktuellen Verfahrensdokumentation betont. Da diese neben den generellen IT-Kontrollen Bestandteil des Basiselements ist, kann ebenfalls keine Beurteilung der Angemessenheit und Wirksamkeit eines GoBD-relevanten Geschäftsprozesses bei einer fehlenden (oder unvollständigen) Verfahrensdokumentation erfolgen.

Eine Prüfung der GoBD-Compliance ist weder verpflichtend noch entfaltet sie gegenüber der Finanzverwaltung eine Bindungswirkung. Allerdings bietet sich eine Prüfung der Wirksamkeit der zur GoBD-Compliance eingerichteten Maßnahmen insb. im Falle von Digitalisierungsprojekten mit Steuerbezug oder aber auch im Vorfeld einer Betriebsprüfung an.

Die Verfahrensdokumentation: Fluch oder Segen – Pflicht oder Kür

Über schwere Mängel und betriebswirtschaftliche Nutzen

Mit den „Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff" (GoBD) hat das Bundesfinanzministerium seine Interpretation der gesetzlichen Anforderungen an eine ordnungsgemäße Buchführung dokumentiert.

Grundsätzlich handelt es sich hierbei lediglich um eine Verwaltungsmeinung, die keinen Gesetzescharakter hat und ausschließlich für Finanzbeamte bindend ist. Im Ergebnis kann demnach jeder Steuerpflichtige eine andere Meinung vertreten. Kommt es dann zum Streit mit den Finanzbehörden, entscheidet in letzter Konsequenz das Finanzgericht.

Gleichwohl haben die wenigsten Steuerpflichtigen ein Interesse an der Beschreitung des Rechtswegs, weshalb in aller Regel versucht wird, der Verwaltungsmeinung zu entsprechen.

Die Verfahrensdokumentation im Fokus

Regelmäßig werden zu Beginn von Prüfungen – sowohl durch Betriebsprüfer als auch durch Wirtschaftsprüfer – Verfahrensdokumentationen (als Bestandteil ordnungsgemäßer Buchführung und begründet mit den GoBD) angefordert.

Die Notwendigkeit des Vorhaltens einer Verfahrensdokumentation ist Ausfluss des Grundsatzes der Nachvollziehbarkeit und der Nachprüfbarkeit (§ 145 Abs. 1 AO, § 238 Abs. 1 S. 2 und S. 3 HGB). Dieser Grundsatz bezieht sich sowohl auf jeden einzelnen Geschäftsvorfall als auch auf das Verfahren insgesamt. Um diese Verfahren ausreichend nachvollziehen zu können, ist eine „aussagekräftige und vollständige Verfahrensdokumentationen, die sowohl die aktuellen als auch die historischen Verfahrensinhalte für die Dauer der Aufbewahrungsfrist nachweist und den in der Praxis eingesetzten Versionen des DV-Systems entspricht" (GoBD Tz. 34), erforderlich.

In Bezug auf den Umfang ist entsprechend GoBD Tz. 151 eine Skalierung möglich, es muss aber gewährleistet sein, dass die Verfahrensdokumentation für einen sachverständigen Dritten – dazu gehören per Definition alle Betriebsprüfer – in angemessener Zeit nachprüfbar ist. In der Praxis werden inzwischen etliche umfangreiche „Musterverfahrensdokumentationen" angeboten. Alleine die „Musterverfahrensdokumentation zur Belegablage" der AWV (Arbeitsgemeinschaft für wirtschaftliche Verwaltung e. V.) hat z. B. einen Umfang von 49 Seiten.

Aufgrund der umfangreichen inhaltlichen Anforderungen ist die Erstellung einer Verfahrensdokumentation zeitaufwendig (nicht zu vergessen die anschließende laufende Aktualisierung). Im Ergebnis schrecken viele Unternehmen hiervor zurück, weswegen eine solche häufig insgesamt fehlt oder zumindest unzureichend ist.

Was bedeutet dies für den Fall einer Betriebsprüfung?

Tatsächlich wird in den GoBD Tz. 155 geregelt, dass soweit eine fehlende oder ungenügende Verfahrensdokumentation die Nachvollziehbarkeit nicht beeinträchtigt, kein formeller Mangel von sachlichem Gewicht vorliegt, der zum Verwerfen der Buchführung führen kann. Es müsste also im Ergebnis ein materieller Verstoß gegen die Ordnungsmäßigkeitsvorschriften der §§ 142 ff. AO vorliegen. Das bloße Fehlen einer Verfahrensdokumentation aber reicht hier nicht aus.

Allerdings muss davon ausgegangen werden, dass die Finanzverwaltung die Tz. 155 nur in Ausnahmefällen anwendet. In der Praxis wird man bei fehlenden bzw. unzureichenden Verfahrensdokumentationen – zumindest – mit Diskussionsbedarf rechnen müssen, der letztlich als Thema in die Schlussbesprechung der Betriebsprüfung eingebracht wird. Zudem ist zu beobachten, dass zumindest für umfassend IT-gestützte Geschäftsprozesse und Abläufe, die steuerrechtlich relevante Daten verarbeiten, eine Verfahrensdokumentation als bindend erachtet wird. Hierzu zählen bspw. die elektronische Dokumentenarchivierung oder auch die Verfahren bei elektronischen Kassensystemen, die zunehmend komplexe und vernetzte IT Systeme darstellen.

Die Konsequenzen aus einer fehlenden Ordnungsmäßigkeit können schwerwiegend sein

Bei schweren formellen Fehlern, die nicht durch anderweitige zumutbare Ermittlungen beseitigt werden können, kann es zu einer Verwerfung der Buchführung in Sinne von § 158 AO kommen. Die Folge einer solchen Verwerfung ist die Schätzung von Besteuerungsgrundlagen gemäß § 162 AO.

Liegen hingegen materielle Mängel bezüglich der Ordnungsmäßigkeit vor, muss zwischen einem unwesentlichen/geringen Umfang an Mängeln und schweren Mängeln differenziert werden:

Bei geringen Mängeln besteht ebenfalls die Gefahr der Hinzuschätzung bzw. eines sog. Sicherheitszuschlags. Eine Verwerfung der Buchführung (insgesamt) nach § 158 AO ist dann aber nicht möglich.

Liegen hingegen schwere materielle Mängel vor, ergeben sich verschiedene Konsequenzen:

- Schätzung nach § 162 AO
- Festlegung von Zwangsmitteln § 328 AO
  - Zwangsgeld § 329 AO bis zu 25.000 Euro. Der Betrag, kann auch mehrfach festgesetzt werden.
  - Ersatzvornahme § 330 AO, d. h. die Finanzbehörde kann auf Kosten des Steuerpflichtigen andere mit der Vornahme von (vertretbaren) Handlungen beauftragen, z. B. das Erstellen von Unterlagen.
  - Unmittelbare Zwangsmaßnahmen § 331 AO. Demnach kann der Steuerpflichtige zu einer Handlung, Duldung oder Unterlassung gezwungen werden. Hierbei handelt es sich um Maßnahmen, wie die Erzwingung von Zutritten oder Herausgabe von Unterlagen.
- Ordnungswidrigkeit § 379 AO mit Geldbußen bis zu 25.000 Euro. Dies gilt insb. in Bezug auf fehlerhafte oder nicht vorhandene Technische Sicherungseinrichtungen bei Kassensystemen.
- leichtfertige Steuerverkürzung (§ 378 AO) mit Geldbußen bis zu 50.000 Euro.
- bei einer GmbH kann es zusätzlich zu einer verdeckten Gewinnausschüttung beim Gesellschafter führen.

Werden Mängel im Rahmen einer Nachschau (Kassennachschau, Umsatzsteuernachschau) festgestellt, kann von Seiten der Finanzbehörden unmittelbar zu einer regulären Betriebsprüfung übergegangen werden.

In diesem Zusammenhang kann im Fall einer fehlenden oder unzureichenden Verfahrensdokumentation nicht davon ausgegangen werden, dass es nur bei einem formellen Fehler bleibt. In vielen Fällen wird zumindest im Rahmen der Schlussbesprechung einer Betriebsprüfung bei (schweren) materiellen Mängeln die Drohung mit entsprechenden Konsequenzen im Raum stehen. Dies führt letztlich dazu, dass eigene Argumentationen in der Diskussion erheblich geschwächt werden.

In letzter Konsequenz…

… gibt es keine Rechtsprechung zur Aufbewahrungspflicht einer Verfahrensdokumentation. Da aber die meisten Unternehmen nicht dazu bereit sein dürften, selbst eine finanzgerichtliche Überprüfung anzustreben, empfiehlt es sich dringend, entsprechende Dokumentationen zu erstellen. Es ist ratsam, an dieser Stelle eben keine Angriffspunkte im Rahmen von Betriebsprüfungen zu bieten.

Darüber hinaus muss betont werden, dass die Erstellung (und Pflege) von Verfahrensdokumentationen in erster Linie nicht den Zweck erfüllen muss, eine Nachvollziehbarkeit und Nachprüfbarkeit für den Betriebsprüfer zu gewährleisten. Vielmehr ergeben Verfahrensdokumentationen tatsächlich einen betriebswirtschaftlichen Sinn, insb. wenn diese inhaltlich eben nicht (nur) für den Steuerprüfer, sondern tatsächlich – wie eigentlich auch gedacht – für die operativen Mitarbeiter des Unternehmens als Unterstützung und Nachschlagewerk geschrieben werden. Dies gilt insb.für den Mittelstand! Hier ist in vielen Fällen das „Kopfwissen" weit verbreitet. D. h., dass bei einem Ausfall Einzelner, wesentliche Prozesse schlicht nicht mehr funktionieren. Gute Verfahrensdokumentationen (insb.) kritischer Prozesse können hier erheblich zur Sicherheit beitragen.

Update von der „Kassen-Front“: EU-Taxameter im Fokus

Erweiterungen ebenso wie Begrenzungen des Anwendungsbereichs der Kassensicherungsverordnung, aber auch ergänzende Anforderungen an Beleginhalte, ergeben sich aus der Verordnung zur Änderung der Kassensicherungsverordnung vom 30.07.2021. Die wichtigsten Änderungen, insb. im Hinblick auf die künftige Notwendigkeit einer TSE für Taxameter, finden Sie in diesem Überblick.

Die relevanten Änderungen treten grundsätzlich am 01.01.2024 in Kraft. Übergangsregelungen und ein abweichender Anwendungszeitpunkt ergeben sich für EU-Taxameter mit INSIKA-Technik (Integrierte Sicherheitslösung für messwertverarbeitende Kassensysteme) bzw. für Wegstreckenzähler im Allgemeinen. Aber beginnen wir am Anfang.

EU-Taxameter und Wegstreckenzähler – jetzt auch „Kassen“

Mit der Verordnung zur Änderung der Kassensicherungsverordnung hat das Bundesfinanzministerium der Finanzen (BMF) eine Anpassung des Geltungsbereiches vorgenommen. Für EU-Taxameter und Wegstreckenzählgeräte ergibt sich danach ebenfalls die Notwendigkeit einer zertifizierten technischen Sicherheitseinrichtung (TSE). Ziel der Änderung bzw. Erweiterung des Geltungsbereiches ist es, die Unveränderbarkeit von digitalen Grundaufzeichnungen ebenfalls bei EU-Taxametern und Wegstreckenzählern durch die TSE sicherzustellen, da Aufzeichnungen bis dato unerkannt gelöscht oder geändert werden konnten.

Per Negativkatalog wird im § 1 der Geltungsbereich der Kassensicherungsverordnung (KassenSichV) für gewisse Systeme explizit eingeschränkt. Aus diesem Negativkatalog wurde mit Änderung der Nr. 6 der Ausschluss von Taxametern und Wegstreckenzählern zurückgenommen. Damit fallen diese nunmehr in den Anwendungsbereich der (neuen) Kassensicherungsverordnung. Zusätzlich wurde mit Aufnahme des § 1 Abs. 2 der Geltungsbereich der Kassensicherungsverordnung explizit um Taxameter sowie Wegstreckenzähler erweitert.

Der grundsätzlich sich unterscheidenden Funktionsweise von Taxametern bzw. Wegstreckenzählern zu anderen „Kassensystemen“ wurde dahingehend Rechnung getragen, dass für diese beiden „Kassen“ gesonderte und explizite Anforderungen zur Transaktion (dem Geschäftsvorfall), zum Beleginhalt sowie hinsichtlich weiterer Spezifika definiert wurden. Diese sind in den §§ 7 bis 10 (KassenSichV n. F.) enthalten.

So hat die Transaktion bei EU-Taxametern neben Zählwerksdaten, allgemeinen Daten, Preisdaten (einer Fahrt) sowie Tarifdaten auch den Zeitpunkt der Beendigung der Betriebseinstellung „Kasse“, eine eindeutige und fortlaufende Transaktionsnummer sowie einen Prüfwert zu enthalten. Die Transaktionsnummer muss so beschaffen sein, dass Lücken in den Transaktionsaufzeichnungen erkennbar sind. Das Ende der Transaktion (Zeitpunkt der Beendigung der Betriebseinstellung „Kasse“), Transaktionsnummer sowie Prüfwert, werden manipulationssicher durch das Sicherheitsmodul festgelegt.

Die hier genannten Angaben zur Transaktion (mit Ausnahme der Tarifdaten) entsprechen zudem den geforderten Mindestinhalten des korrespondierenden Belegs. Die Mindestinhalte werden diesbezüglich noch um die Seriennummer des Sicherheitsmoduls erweitert. Daneben gelten die allgemeinen Anforderungen an einen Beleg hinsichtlich seiner Lesbarkeit (gemäß § 6 Sätze 2 bis 4 KassenSichV).

Analoge Anforderungen an die Transaktion gelten beim Einsatz eines Wegstreckenzählers unter Berücksichtigung der hier nicht relevanten Tarifdaten sowie die für Taxameter spezifische Betriebseinstellung „Kasse“. Die geforderten Beleginhalte sind ebenfalls analog für Wegstreckenzähler anzuwenden, wobei bei Wegstreckenzählern der Beleg durch eine dem Gesetz entsprechende Aufzeichnung des Geschäftsvorfalls ersetzt werden kann, wenn keine digitale Schnittstelle vorhanden ist.

Wie eingangs bereits erwähnt, ist eine Übergangsregelung zur Umsetzung der Anforderungen für EU-Taxameter mit INSIKA-Technik vorgesehen. Soweit ein EU-Taxameter vor dem 01.01.2021 mit dieser Technik ausgerüstet wurde (wodurch bereits eine gewisse Sicherheitsstufe hinsichtlich des Schutzes vor unprotokollierten Änderungen und Löschung von Grundaufzeichnungen erreicht wurde), ist der neu gefasste § 7 KassenSichV für diese EU-Taxameter erst ab dem 01.01.2026 anzuwenden. Damit ergibt sich in diesem Fall eine Fristverlängerung zur Umrüstung von zwei Jahren. Die Erfüllung der Voraussetzung zur Inanspruchnahme dieser Fristverlängerung ist aber dem zuständigen Finanzamt bis zum 31.01.2024 mitzuteilen.

Hingegen ist der Anwendungszeitpunkt für Wegstreckenzähler erst noch durch das BMF bekannt zu geben. Dieser tritt erst ein, sobald mindestens drei voneinander unabhängige Unternehmen Wegstreckenzähler am Markt anbieten, die über eine geeignete digitale Schnittstelle im Sinne der KassenSichV verfügen, und zudem eine Konformitätsbewertungsstelle nach § 13 oder § 14 des Mess- und Eichgesetzes die Konformität dieser dann angebotenen bzw. verfügbaren Wegstreckenzähler mit den Anforderungen des Mess- und Eichgesetzes feststellt. Ab diesem Zeitpunkt sind dann o. g. Anforderungen an neu in den Verkehr gebrachte Wegstreckenzähler umzusetzen.

Der Vollständigkeit halber sei noch erwähnt, dass im Zuge der Erweiterung des Anwendungsbereichs der KassenSichV eine gleichzeitige Begrenzung des Anwendungsberei-

ches erfolgt ist. Kassen- und Parkscheinautomaten wurden aufgrund der Vergleichbarkeit zu Fahrscheindruckern, ebenso wie Ladepunkte für Elektro- oder Hybridfahrzeuge, von dem Anwendungsbereich der KassenSichV ausgenommen.

Protokollierung und Mindestinhalte eines Belegs

Hinsichtlich der Protokollierung von digitalen Grundaufzeichnungen ergibt sich eine Erweiterung der notwendigen Angaben in Bezug auf die Transaktion (Aufzeichnung eines (eindeutigen) Geschäftsvorfalls). War bisher die Angabe der Seriennummer des elektronischen Aufzeichnungssystems, alternativ die Seriennummer des Sicherheitsmoduls, im Rahmen einer Transaktion zu erfassen (und zu protokollieren), sind nun beide Seriennummern zu protokollieren.

Mit der Anpassung der zu protokollierenden Inhalte einer Transaktion ergeben sich ebenfalls Anpassungen der Anforderungen an Mindestinhalte des Belegs. Auch hier ist künftig die Seriennummer des Sicherheitsmoduls nicht als Alternative, sondern als Mindestinhalt neben der Seriennummer des elektronischen Aufzeichnungssystems anzugeben. Zusätzlich wird als Mindestangabe auf dem Beleg der Prüfwert (im Sinne des § 2 Satz 2 Nr. 7 KassenSichV) sowie der fortlaufende Signaturzähler definiert, welcher vom Sicherheitsmodul festgelegt wird.

Für die Ausgabe von Belegen ergibt sich nun auch eine ressourcenschonende Alternative, im Sinne einer Reduzierung der Beleggröße. Mit Neufassung bzw. Erweiterung des § 6 KassenSichV besteht die Möglichkeit, die geforderten Mindestinhalte eines Belegs mittels QR-Codes auslesbar zu machen. Dadurch kann der Beleg verkürzt und damit Kosten sowie Ressourcen gespart werden.

Umfassende Änderungen im Kaufrecht für Onlinehandel und digitale Inhalte

Der Gesetzgeber ist im Sommer 2021 seinen Umsetzungspflichten aus diversen EU-Richtlinien nachgekommen und hat verschiedenste Gesetze auf den Weg gebracht, die insb. den eCommerce und Geschäfte mit Verbrauchern betreffen. Aufgrund der Fülle von Regelungen, fällt es schwer, den Überblick zu behalten, welche Maßnahmen wann getroffen werden müssen. Hierfür bleibt zum Teil nur wenig Zeit.

Deutschland ist diesen Sommer in letzter Minute seinen Umsetzungspflichten aus diversen EU-Richtlinien nachgekommen und hat das Verbraucherrecht umfassend angepasst. Die Neuregelungen im Bürgerlichen Gesetzbuch (BGB), dem Einführungsgesetz zum Bürgerlichen Gesetzbuch (EGBG) und dem Gesetz zum unlauteren Wettbewerb (UWG) sind weitreichend und verlangen insb. von Onlinehändlern diverse Anpassungen.

Einwilligung in Telefonwerbung und Abtretungsverbot

Bereits zum 01.10.2021 wurden zwei wichtige Punkte umgesetzt. So sind zum einen Regelungen in AGB unwirksam, die ein Abtretungsverbot von Geldforderungen enthalten. Damit soll dem Verbraucher ermöglicht werden, seine Forderungen auch an Dritte zur Rechtsdurchsetzung verkaufen zu können.

Zum anderen treten verschärfte Regelungen zur Dokumentationspflicht bzgl. Telefonwerbung in Kraft. Dass für Werbung mittels Telefonanrufes eine ausdrückliche Einwilligung des Verbrauchers notwendig ist, ist bereits lange bekannt. Gesetzlich konkret neu geregelt ist jetzt, dass diese ausdrückliche Einwilligung dokumentiert und fünf Jahre aufbewahrt werden muss, andernfalls droht ein Bußgeld von bis zu 50.000 Euro.

Änderungen des Kaufrechts – insb. Gewährleistungsrecht und Verbrauchsgüterkauf

Eine der umfassendsten Gesetzesänderungen betrifft das Kaufrecht. Ab 01.01.2022 wird für alle Kaufverträge ein neuer Mangelbegriff gelten und es werden neue Regeln zur Gewährleistung – insb. im Verbrauchsgüterkauf – in Kraft treten.

Für die Mangelfreiheit kommt es künftig darauf an, ob die Kaufsache den „subjektiven und objektiven Anforderungen sowie den Montageanforderungen" entspricht. Von Relevanz werden dabei in Zukunft auch von Gesetzes wegen die Beschaffenheit von etwaigen Proben und Mustern, aber auch von Zubehör, Montageanleitungen und Werbeaussagen (bspw. des Herstellers) sein.

Für Vertragsbeziehungen mit Verbrauchern gelten künftig diverse Erleichterungen im Gewährleistungsfall. Bspw. profitiert der Käufer ab 2022 von einer auf ein Jahr verlängerten Beweislastumkehr, dass die Sache bereits bei Übergabe mangelhaft war. Daneben wurden die Voraussetzungen für den Rücktritt oder die Geltendmachung eines Schadensersatzanspruchs aufgeweicht. So muss der Verbraucher häufig keine konkrete Frist mehr setzen, bevor er vom Kaufvertrag zurücktreten oder Schadensersatz verlangen kann.

Sache mit digitalen Elementen – Aktualisierungspflicht der Verkäufer

Entsprechend der EU-Richtlinien wird das deutsche BGB – insb. das Gewährleistungsrecht – nun auch an die speziellen Anforderungen der Digitalisierung angepasst. Neu eingefügt werden Regelungen für „Kaufsachen mit digitalen Elementen". Hervorzuheben ist hierbei insb. die neu normierte Aktualisierungspflicht, bei deren Verletzung die Kaufsache als mangelhaft gilt.

Das bedeutet, dass auch eine ursprünglich mangelfreie Kaufsache im Laufe der Zeit mangelhaft wird, sofern der Verkäufer nicht oder nicht rechtzeitig Updates liefert. Davon umfasst sind sowohl funktionserhaltende als auch Sicherheitsaktualisierungen. Dabei soll die Dauer der Aktualisierungspflicht von den Umständen des Einzelfalls abhängen. Sie wird je nach Art des Produkts und dem Erwartungshorizont des Durchschnittskäufers bemessen. Es ist demnach offen, ab wann ein Verkäufer nicht mehr zur Aktualisierung verpflichtet ist.

Der Verkäufer, der nicht zugleich Hersteller der Produkte ist, muss deshalb künftig in seinen Lieferverträgen besonders darauf achten, diese Pflicht zur Bereitstellung von Updates abzudecken, um ggfs. Regressansprüche geltend machen zu können.

Neue Regelungen für Verträge mit digitalen Produkten

Ab Januar 2022 gelten zudem neue Regelungen für Verträge, die die „Bereitstellung digitaler Inhalte und digitaler Dienstleistungen" (zusammen „digitale Produkte") zum Gegenstand haben. Davon betroffen sind insb. Anbieter von Apps, eBooks und Streaming-Diensten, aber auch Cloud-Anbieter und Betreiber sozialer Netzwerke.

Eine der wichtigsten Neuerungen ist dabei, dass ein Vertrag schon dann als „entgeltlich" gilt, sobald der Verbraucher sich zur Bereitstellung seiner Daten verpflichtet, die über die ausschließliche Verwendung zur Vertragsdurchführung hinaus gehen. „Bezahlt" der Verbraucher also die Leistung mit seinen Daten, ist künftig das Widerrufsrecht auf diese Verträge anwendbar.

Darüber hinaus gelten auch für die Verträge zu digitalen Produkten spezielle Regelungen im Gewährleistungsrecht, die sich an denen des neuen Kaufrechts orientieren.

Strenge Anforderungen an Vertragslaufzeiten und Verlängerungen

Ab März 2022 gelten verschärfte Bedingungen für Vertragslaufzeiten, deren automatische Verlängerung sowie deren Kündigung.

Verträge dürfen nach einer Mindestlaufzeit von maximal zwei Jahren künftig nur noch auf unbestimmte Zeit mit einmonatiger Kündigungsmöglichkeit verlängert werden. Eine bislang häufig anzutreffende Praxis über die Verlängerung um ein weiteres Jahr ist damit nicht mehr zulässig, da der Kunde nicht darauf beschränkt werden darf, erst zum Ende der automatischen Verlängerung zu kündigen. Auch wird die Kündigungsfrist von maximal drei Monaten auf einen Monat verkürzt.

Findet der Vertragsschluss im Internet statt, hat der Unternehmer ab Juli 2022 auch einen sog. „Kündigungsbutton" vorzuhalten. Über diese Schaltfläche soll der Kunde künftig einfacher seinen Vertrag beenden können.

Umfassende Transparenzpflichten für Online-Marktplätze

Zusätzlich hat der Gesetzgeber Handlungsbedarf bei der Transparenz auf Online-Marktplätzen, wie bspw. Amazon, eBay, etsy & Co, gesehen.

Ähnlich wie beim Ranking von Suchergebnissen, haben Marktplatzbetreiber ab 28.05.2022 konkrete Angaben zu Ranking-Kriterien und deren Gewichtung zu machen. Darüber hinaus sind die Käufer ausdrücklich über die Verbraucher- oder Unternehmereigenschaft zu informieren. Insb. Amazon dürfte auch Anlass zur Regelung gegeben haben, dass nunmehr wirtschaftliche Verflechtungen zwischen der Plattform und etwaigen Verkäufern offenzulegen sind.

Achtung bei Preisbildung über Profiling oder Werbung mit Preisreduktion

Ebenfalls zum 28.05.2022 müssen alle Verkäufer ausdrücklich Angaben machen, sofern sie für die Preisbildung eine automatisierte Entscheidungsfindung, sog. „Profiling", verwendet haben.

Ebenso muss bei der Werbung mit Preisreduzierungen als vorheriger Preis immer der günstigste Preis der letzten 30 Tage mit angegeben werden. Dies dürfte insb. bei zeitlich nahe aufeinander fallenden Verkaufsanlässen, wie bspw. Black Friday und dem Weihnachtsgeschäft, relevant werden.

Hinweis: Für Onlinehändler wird das Jahr 2022 zur besonderen Herausforderung, da sowohl AGB als auch Datenschutzerklärungen, Widerrufsbelehrungen und Preisangaben zu unterschiedlichen Zeitpunkten – teilweise sogar mehrfach – anzupassen sind, wobei erste Anpassungen schon jetzt unmittelbar anstehen.

Darüber hinaus haben die Änderungen des Kauf- und Gewährleistungsrechts Auswirkungen auf Lieferverträge und etwaige Regressansprüche im B2B-Geschäftsverkehr, die künftig zu beachten sind.

KritisV 2.0 – Die große Erweiterung der Kritischen Infrastrukturen?

Hintergrund IT-Sicherheitsgesetz 2.0:

Zum Schutz der Funktionsfähigkeit Kritischer Infrastrukturen sieht das BSI-Gesetz (BSIG) vor, dass die Betreiber der Kritischen Infrastrukturen ihre IT-Systeme durch angemessene organisatorische und technische Vorkehrungen absichern müssen. Kritische Infrastrukturen im Sinne des BSI-Gesetzes sind Einrichten, Anlagen oder Teile davon aus den folgenden Sektoren:

In der BSI-Kritis-Verordnung (BSI-KritisV), die die Konkretisierung des IT-Sicherheitsgesetzes darstellt, werden die exakten Schwellenwerte für Kritische Infrastrukturen definiert. Ein Schwellenwert stellt laut § 1 der BSI-KritisV einen Wert dar, bei dessen Erreichen oder dessen Überschreitung der Versorgungsgrad einer Anlage oder Teilen davon als bedeutend im Sinne von § 10 Abs. 1 Satz 1 des BSI-Gesetzes anzusehen ist.

Unternehmen, die mit ihrer Anlage die Schwellenwerte als Kritische Infrastruktur nach KritisV überschreiten, fallen als Kritis-Betreiber unter die Kritis-Regulierung nach dem IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0). Somit unterliegen die Unternehmen den folgenden Cyber Security-Pflichten:

1. Selbständige Einstufung als Kritis-Betreiber durch das Unternehmen anhand der Schwellenwerte
2. Registrierung der Anlagen als Kritis beim BSI
3. Kritis-Meldepflichten für IT-Störungen, Angriffe und Vorfälle der betroffenen Anlagen ans BSI
4. Festlegung/Abgrenzung des Umfangs der kritischen Anlage, d. h. Festlegung des Scopes im Unternehmen
5. Einrichtung der technischen und organisatorischen Maßnahmen zum Management von IT-Sicherheit (ISMS), Risiken, Kontinuität (BCMS) und Technologien
6. Prüfung der Umsetzung der Kritis-Anforderungen durch einen externen Kritis-Prüfer und Meldung der Ergebnisse an das BSI.

KritisV 2.0:

Am 18.08.2021 hat das Bundeskabinett die „Zweite Verordnung zur Änderung der BSI-Kritis-Verordnung" beschlossen. Diese tritt bereits zum 01.01.2022 in Kraft und beinhaltet wesentliche Änderungen, auf die sich zukünftige Betreiber kritischer Infrastrukturen (Kritis) einstellen müssen. Grundsätzlich handelt es sich bei den Änderungen im Wesentlichen um das Ergebnis der in § 9 KritisV definierten Evaluation. Es wurden jedoch keine wesentlichen Erweiterungen oder Anpassungen, wie bspw. die Einführung des neuen Sektors Siedlungsabfallentsorgung oder die „Unternehmen im Besonderen öffentlichen Interesse" aus dem IT-Sicherheitsgesetz 2.0, getroffen. Diese Erweiterungen und Anpassungen werden durch eine weitere Änderung der KritisV erfolgen.

Zusammenfassung der Kennzahlen

Durch die umgesetzten Änderungen werden voraussichtlich 252 neue Kritis-Betreiber zu den bereits bestehenden circa 1.600 Betreibern hinzukommen. Der größte Zuwachs wird in dem **Sektor Energie** erwartet. Hier werden voraussichtlich

- 131 neue Betreiber in der Anlagenkategorie Strom,
- 13 Betreiber in der Anlagenkategorie Gas und
- vier Betreiber in der Anlagenkategorie Mineralöl

erwartet.

Der zweitgrößte Zuwachs dürfte im **Sektor Transport und Verkehr** zu verzeichnen sein. Durch die Änderungen werden

- sechs neue Betreiber im Sektor Luftverkehr,
- 34 neue Betreiber im Sektor Schifffahrt sowie
- 34 neue Betreiber im Sektor Straßenverkehr

erwartet.

In der **Anlagenkategorie ÖPNV** wird mit keinem Zuwachs an neuen Betreibern gerechnet. Für den **Sektor Gesundheit** wurden im Entwurf keine Zahlen veröffentlicht – somit ist der Zuwachs hier noch ungewiss.

Mit kleinerem Zuwachs wird in den **Sektoren Informationstechnik und Telekommunikation** sowie **Finanz- und Versicherungswesen** gerechnet. Im **Sektor Finanz- und Versicherungswesen** sollen aufgrund der Aufnahme neuer Anlagen 21 neue Betreiber in der Anlagenkategorie Handel hinzukommen. Im **Sektor Informationstechnik und Telekommunikation** wird durch die Aufnahme neuer Anlagen sowie die Änderung von Schwellwerten 10 neue Kritis-Betreiber erwartet. Die genannten Zuwächse lassen sich auf die folgenden Änderungen zurückführen:

Überblick über die Änderungen der übergreifenden Definitionen

Auffällig ist, dass bereits in dem Allgemeinen Teil der BSI-KritisV Änderungen an den Definitionen vorgenommen wurden. Bspw. fallen nach § 1 Abs 1 Nr. 1c KritisV nun auch Software und IT-Dienste unter die Anlagendefinition. Ebenfalls wird in § 1 Abs 2 KritisV nun auch der Begriff der gemeinsamen Anlage konkretisiert: „Mehrere Anlagen derselben Kategorie, die durch einen betriebstechnischen Zusammenhang verbunden sind, gelten als gemeinsame Anlage, wenn sie gemeinsam zur Erbringung derselben kritischen Dienstleistung notwendig sind.". Somit ist kein rechtlicher Spielraum hinsichtlich der Auslegung einer Anlage sowie einer gemeinsamen Anlage gegeben.

Ebenfalls wird in § 1 Abs 2 KritisV die Verantwortlichkeit definiert, wenn eine Anlage von zwei oder mehr Personen betrieben wird. In diesem Fall ist jeder für die Erfüllung der Pflichten als Betreiber verantwortlich.

Mit der neuen BSI-KritisV wird die Definition zum Ende des Geltungsbereichs der Verordnung eingeführt. Dies erfolgt in den einzelnen Anhängen der BSI-KritisV, ist jedoch in jedem Anhang und somit in jedem Sektor gleich definiert worden. „Nicht mehr als Kritische Infrastruktur gilt eine solche Anlage ab dem 01.04. des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den genannten Schwellenwert unterschreitet." (bspw. Anhang 1 Teil 1 Nr. 3). Fällt eine Anlage bspw. im Kalenderjahr 2021 unter die genannten Schwellenwerte, nachdem es im Kalenderjahr 2020 diese noch überschritten hat, fällt die Anlage ab dem 01.04.2022 nicht mehr unter die Verordnung.

Überblick über die Änderungen der Anlagenkategorien

In der neuen BSI-KritisV wurden neben den Definitionen auch Änderungen an den Anlagenkategorien vorgenommen. Insgesamt wurden 17 Anlagenkategorien hinzugefügt und fünf Anlagenkategorien gelöscht. Somit ist ein genereller Zuwachs an Anlagenkategorien erfolgt.

Neu hinzugekommen sind u. a. folgende Anlagenkategorien:

1. Energie

a. Anlagen zur zentralen standortübergreifenden Steuerung im Bereich der Gasversorgung (Anhang 1 Teil 3 Nr. 2.1.2)

b. Gasgrenzübergabestellen (Anhang 1 Teil 3 Nr. 2.2.2)

c. Gashandelssysteme (Anhang 1 Teil 3 Nr. 2.4.1)

d. Anlagen zur zentralen standortübergreifenden Steuerung im Bereich der Erdölförderung und Produktherstellung (Anhang 1 Teil 3 Nr. 3.1.3)

e. Mineralölhandel (Anhang 1 Teil 3 Nr. 3.4.1)

f. Anlagen zur zentralen standortübergreifenden Steuerung im Bereich der Fernwärmeversorgung (Anhang 1 Teil 3 Nr. 4.3.1)

2. Wasser

a. Durch Neudefinition der Gewinnungsanlage fallen nun auch Stauanlagen unter den Begriff Gewinnungsanlage (Anhang 2 Teil 1 Nr. 1.1)

3. IT

a. Top-Level-Domain-Name-Registry (Anhang 4 Teil 3 Nr. 1.4.3)

4. Gesundheit

a. Labore im Bereich der Laboratoriums Diagnostik (Anhang 5 Teil 3 Nr. 4.1)

b. Laborinformationsverbund im Bereich der Laboratoriums Diagnostik (Anhang 5 Teil 3 Nr. 4.2)

5. Finanz- und Versicherungswesen

a. System für das Erzeugen von Aufträgen zum Handel von Wertpapieren und Derivaten und Weiterleiten an einen Handelsplatz im Bereich der Erbringung von Aufträgen in den Handel (Anhang 6 Teil 3 Nr. 4.4.1)

b. System eines Handelsplatzes im Bereich der Ausführung des Handels (Anhang 6 Teil 3 Nr. 4.5.1)

c. Sonstige Depotführungssysteme für die Bestandsführung für den Kunden (Anhang 6 Teil 3 Nr. 4.6.1)

6. Transport und Verkehr

a. Verkehrszentrale einer Fluggesellschaft im Luftverkehr im Bereich Personen- und Güterverkehr (Anhang 7 Teil 3 Nr. 1.1.5)

b. Flughafenleitorgan im Luftverkehr im Bereich Personen- und Güterverkehr (Anhang 7 Teil 3 Nr. 1.1.5)

c. Hafenleitungsorgan (nur Güterverkehr) in der See- und Binnenschifffahrt (Anhang 7 Teil 3 Nr. 1.3.4)

d. Umschlaganlagen in See- und Binnenhäfen (Anhang 7 Teil 3 Nr. 1.3.5)

e. Intelligentes Verkehrssystem im Straßenverkehr (Anhang 7 Teil 3 Nr. 1.4.3)

Folgende Anlagenkategorien wurden gestrichen:

1. Energie:

a. Erzeugungsanlage mit Wärmeauskopplung (KWK-Anlage) im Bereich der Stromversorgung (ehem. Anhang 1 Teil 3 Nr. 1.1.2)

b. Messstelle im Bereich der Stromversorgung (ehem. Anhang 1 Teil 3 Nr. 1.3.2)

2. Gesundheit

a. Transportsystem im Bereich der Laboratoriumsdiagnostik (ehem. Anhang 5 Teil 3 Nr. 4.1.1)

b. Kommunikationssystem zur Auftrags- oder Befundübermittlung im Bereich der Laboratoriumsdiagnostik (ehem. Anhang 5 Teil 3 Nr. 4.1.2)

3. Transport und Verkehr

a. Verkehrssteuerungs- und Leitsystem des ÖPNV (ehem. Anhang 7 Teil 3 Nr. 1.5.2)

Überblick über die der Schwellenwerte

Neben den Änderungen an den Anlagenkategorien wurden auch Änderungen an Schwellenwerten von bestehenden Anlagenkategorien beschlossen. Dazu zählt u. a. die Senkung der folgenden Schwellenwerte:

1. Energie:

a. Senkung des Schwellenwertes für Erzeugungsanlagen von 420 auf 104 MW installierte Nettonennleistung (Anhang 1 Teil 3 Nr. 1.1.1)

b. Senkung des Schwellenwertes für Erzeugungsanlagen, wenn diese als Schwarzanlage nach § 3 Abs. 2 des Beschlusses BK-18-249 kontrahiert ist, von 420 auf 0 MW installierte Nettonennleistung (Anhang 1 Teil 3 Nr. 1.1.1)

c. Senkung des Schwellenwertes für Erzeugungsanlagen zur Erbringung von Primärregelleistung nach § 2 Nr. 8 StromNZV präqualifiziert von 420 auf 36 MW (Anhang 1 Teil 3 Nr. 1.1.1)

d. Senkung der Schwellenwerte für Anlage oder Systeme zum Betrieb eines Logistikzentrums in den Segmenten Massengut-, Ladungs-, Stückgut-, Kontrakt-, See- oder Luftfrachtlogistik nach der oben genannten Unterteilung auf dieselben Schwellenwerte (Anhang 1 Teil 3 Nr. 1.1.2)

e. Senkung des Schwellenwertes für zentrale Anlagen oder Systeme für den Stromhandel von 200 TWh/Jahr auf 3,7 TWh/Jahr

2. IT:

a. Senkung des Schwellenwertes für IXP von 300 auf 100 angeschlossene autonomer Systeme (Jahresdurchschnitt) (Anhang 4 Teil 3 Nr. 1.3.1)

b. Senkung des Schwellenwertes für Rechenzentren von 5 auf 3,5 MW vertraglich vereinbarte Leistung (Anhang 4 Teil 3 Nr. 2.1.1)

c. Senkung des Schwellenwertes für Serverfarmen (Hosting) von 25.000 auf 10.000 für den Nutzer betriebene physische Instanzen im Jahresdurchschnitt oder 15.000 für den Nutzer betrieben virtuelle Instanzen im Jahresdurchschnitt (Anhang 4 Teil 3 Nr. 2.2.1)

Demgegenüber dazu wurde der Schwellenwert für Logistikanlagen (Anlage oder System zum Betrieb eines Logistikzentrums in den Segmenten Massengut-, Ladungs-, Stückgut-, Kontrakt-, See- oder Luftfrachtlogistik, Anhang 7 Teil 3 Nr. 1.6.1) von 17 Mio. Tonnen im Jahr auf 17,55 Mio. Tonnen im Jahr erhöht.

Neben den Senkungen und den Erhöhungen wurden neue Schwellenwerte für bestehende Anlagen definiert. Dazu zählt bspw. im Sektor Energie die Aufnahme des Schwellenwertes hinsichtlich Flugkraftstoff. Dies betrifft alle Anlagenkategorien im Bereich der Kraftstoff- und Heizölversorgung (Anhang 1 Teil 3 Punkt 3). Der Schwellenwert wurde Anlagenkategorie übergreifend auf 63.750 Tonnen/Jahr definiert. Ebenfalls als neuer Schwellenwert wurde bspw. die Anzahl der Sendungen pro Jahr im Sektor Transport und Verkehr für die Anlagenkategorie Logistik (Anhang 7 Teil 3 Nr. 1.6) definiert.

In Zusammenhang mit den Änderungen der Anlagenkategorien und der Schwellenwerte mussten ebenfalls einige Definitionen in den einzelnen Sektoren angepasst werden. Diese korrespondieren mit den oben aufgeführten Änderungen im Bereich der Anlagenkategorien und Schwellenwerten und sind jeweils im Teil 2 des jeweiligen Anhanges dargelegt.

Vergleich zum IT-SiG 2.0

Das IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) ist am 28.05.2021 in Kraft getretenen. Im Zuge dessen ist der Anwendungsbereich des BSIG um sog. „Unternehmen im besonderen öffentlichen Interesse" (UBI/UNBÖFI) erweitert worden. Hierbei handelt es sich um Unternehmen, die von „erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind oder die für solche Unternehmen als Zulieferer wegen ihrer Alleinstellungsmerkmale von wesentlicher Bedeutung sind" (vgl. § 2 Abs. 14 Satz 1 Nr. 2 BSIG). Diese setzen sich aus den folgenden drei Gruppen zusammen:

1. Rüstung
2. Volkswirtschaftliche Bedeutung
3. Gefahrenstoffe.

Auf die betroffenen Unternehmen kommen mit dem neuen § 8 f. UBI/UBÖFI-Pflichten für Cyber Security zu:

a. Identifikation und Registrierung
b. Selbsterklärung IT-Sicherheit
c. Vorfallsmeldungen.

In diesem Zusammenhang spricht man auch von den „Kritis-Light". Die Definition der „UBI"/"UBÖFI", deren Anlagen und Schwellenwerte sowie Fristen sind jedoch nicht in der KritisV 2.0 definiert worden.

Darüber hinaus wurden die BSI-KritisV um den Sektor „Siedlungsabfallentsorgung" (§ 2 Abs. 10 BSIG) erweitert, wodurch nun u. a. Entsorger zur Kritischen Infrastruktur gehören (Dienstleistung Entsorgung von Siedlungsabfällen mit Sammlung, Beseitigung und Verwertung). Analog der UBI/UBÖFI sind in der KritisV weder die Definition der „Siedlungsabfälle", deren Anlagen, Schwellenwerten oder Fristen definiert worden. Dies ist derzeit jedoch ebenfalls noch ausstehend.

Nach dem IT-SiG 2.0 sind ab 2023 für die Kritis-Anlagen Prozesse und Technologien notwendig, um Angriffe und Störungen zu erkennen und darauf in der Cyber Defense reagieren zu können. Nach § 8a Abs. 1a BSIG „umfasst [die Verpflichtung] ab dem 01.05.2023 auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen.". Diese Konkretisierung wurde in der KritisV nicht weitergehend definiert oder ausgeführt. Dies muss jedoch im Rahmen des Betriebes einer Kritischen Infrastruktur berücksichtigt werden.

Kritische Bewertung der Änderungen

An der neuen Verordnung ist u. a. zu kritisieren, dass an dem Regelschwellenwert von 500.000 versorgten Personen trotz fehlender Transparenz in dessen Ausarbeitung weiterhin festgehalten wird. Der Regelschwellenwerte von 500.000 Personen ist vor allem in den Sektoren Energie und Wasserversorgung unverständlich, da somit weiterhin nicht einmal viele der Stadtwerke in deutschen Großstädten Berücksichtigung finden.

Hinsichtlich der erweiterten Anlagen-Definition um Software und IT-Dienste ist zusätzlich zu bemängeln, dass die Kritikalität nicht als Entscheidungskriterium in die Verordnung Einfluss fand, dies aber anzunehmen ist, da sonst ein Fass ohne Boden entstehen würde. Es bedarf der Klarstellung, dass es sich beim neuen Anlageverständnis lediglich um die Software / IT-Dienste handelt, die tatsächlich für die Erbringung der kritischen Dienstleistung notwendig sind, also um fachspezifische Anwendungssoftware / IT-Dienste mit hoher Kritikalität.

Die Regularien müssen insgesamt zum Rest der deutschen Gesetzgebung passen und europaweit unbedingt harmonisiert werden. Dies gilt insb. im Hinblick auf derzeit auf EU-Ebene diskutierte sektorübergreifende und sektorspezifische Legislativvorhaben (NIS2, RCE, DORA). Hier greift der Entwurf in Teilen vor und könnte einer EU-weiten Harmonisierung der Sicherheitsstandards ein Stück weit entgegenstehen bzw. zu erheblichen Kosten und Mehraufwänden durch Doppelregulierungen führen.

Fazit

Die nun erfolgten Änderungen machen eines klar: IT-Sicherheit gewinnt immer mehr an Bedeutung, weswegen auch der Kritis-Anwendungsbereich weiter ausgeweitet wird. Es sind bereits einige, tiefgreifende Änderungen erfolgt, der große Umschwung durch die Definition neuer Sektoren ist jedoch ausgeblieben. Auch weiterhin sind die Regelschwellwerte und damit die Berechnungsgrundlagen einiger Schwellwerte undurchsichtig. Betroffene Anlagenbetreiber sollten daher frühzeitig klären, inwieweit auch sie von den Änderungen betroffen werden, um sich schnell und effektiv auf die neue Situation einstellen zu können. Da die Änderungen bereits zum 01.01.2022 in Kraft treten, gelten bereits für die Meldung im April 2023 für das Geschäftsjahr 2022 die angepassten Schwellenwerte. Eine zeitnahe Prüfung der neuen Schwellenwerte ist somit dringend empfohlen.

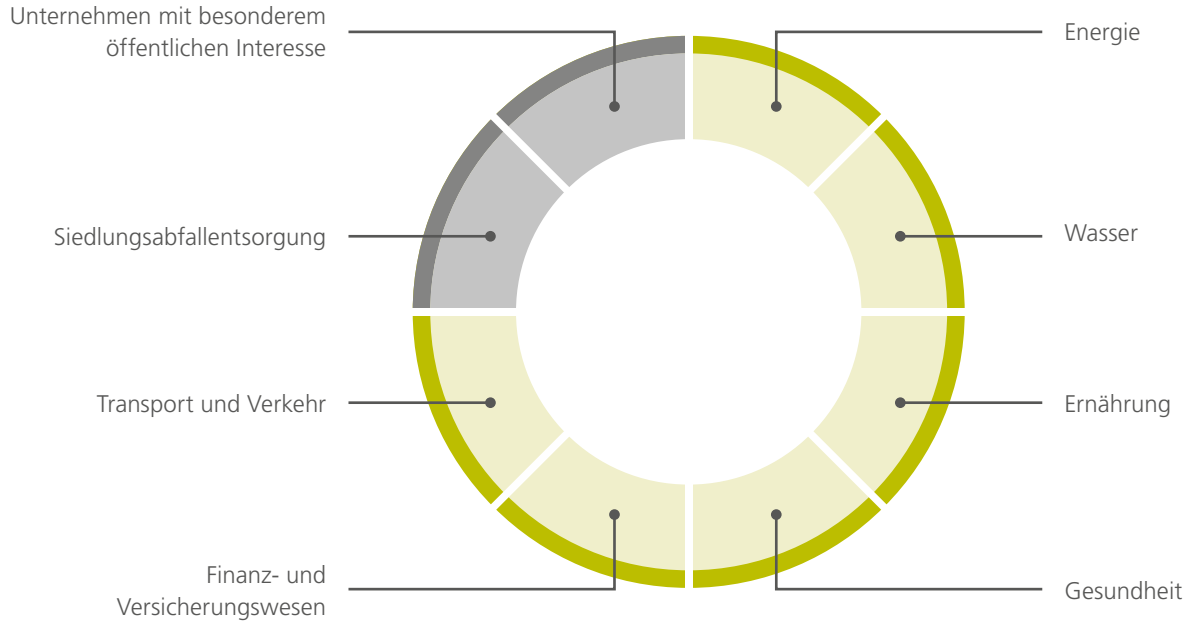


Schaubild: Sektoren

Implementierung und Zertifizierung des Compliance-Management-Systems: Die neue ISO 37301 als Alternative zum IDW PS 980

Ziel einer ganzheitlichen Compliance-Steuerung ist die Umsetzung und Einhaltung von gesetzlichen und regulatorischen Anforderungen, um einen verantwortungsvollen und sicheren Umgang mit sämtliche Compliance-relevanten Aspekten zu gewährleisten. Der Anforderungsrahmen reicht dabei u. a. von der Informationssicherheit über Datenschutz und IT-Sicherheit, wirtschafts- und steuerrechtlichen Anforderungen bis zum Aufbau und Umsetzung des Internen Kontrollsystems.

Ein Compliance-Management-System muss insgesamt gesetzliche und vertragliche Vorgaben wie auch interne und externe Compliance-Vorgaben von externen Dritten (z. B. Kunden oder Lieferanten) berücksichtigen. Die Compliance-Steuerung umfasst neben der Identifikation der relevanten Vorgaben auch die Konzeption, Umsetzung und Überwachung der Anforderungen.

Das heißt ein ganzheitliches Compliance-Management-System (CMS) geht weit über die reine Selbstverpflichtung der Einhaltung formaler Gesetze hinaus. Wenngleich diesem Begriff keine Legaldefinition zugrunde liegt, versteht man darunter die Gesamtheit aller Prozesse und Maßnahmen zur Einhaltung sämtlicher Regeln einschließlich freiwilliger Unternehmens-Kodizes.

Das Institut der Wirtschaftsprüfer in Deutschland e. V. (IDW) definiert das CMS als „die auf der Grundlage der von den gesetzlichen Vertretern festgelegten Ziele eingeführten Grundsätze und Maßnahmen eines Unternehmens […], die auf die Sicherstellung eines regelkonformen Verhaltens der gesetzlichen Vertreter und der Mitarbeiter des Unternehmens sowie ggf. von Dritten abzielen, d. h. auf die Einhaltung bestimmter Regeln und damit auf die Verhinderung von wesentlichen Verstößen".

Ein (gelebtes) CMS birgt über den ursächlichen Zweck hinaus, die Einhaltung der relevanten Compliance-Anforderungen zu prüfen und sicherzustellen, weitere Potenziale, wie etwa eine damit einhergehende Effizienzsteigerung. Die Implementierung eines CMS verschafft einen umfassenden Überblick über mögliche Compliance-Risiken und dadurch die Möglichkeit, diesen zeitnah mit angemessenen Maßnahmen begegnen oder bestenfalls zuvorkommen zu können. Zudem wird die Einhaltung der kundenseitigen Compliance-Anforderungen begünstigt. Schließlich kann der Nachweis über ein eingerichtetes und gelebtes CMS Vertrauen und letztlich auch einen Reputationsgewinn schaffen.

Der IDW PS 980

Seit dem Jahr 2011 stellt das IDW mit dem Prüfungsstandard IDW (PS) 980 einen Standard zur Verfügung, anhand dessen ein implementiertes CMS in drei Stufen, konkret der Konzeption, der Angemessenheit sowie der Wirksamkeit geprüft und testiert werden kann. Geprüft wird im Rahmen dessen laut Prüfungsstandard, „ob die in der CMS-Beschreibung enthaltenen Aussagen zur Konzeption des CMS in allen wesentlichen Belangen angemessen dargestellt sind." Gegenstand der zweiten Prüfungsstufe ist die Eignung der Grundsätze und Maßnahmen, um „mit hinreichender Sicherheit sowohl Risiken für wesentliche Regelverstöße rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern." Zudem wird im Rahmen dieser Prüfung auch untersucht, ob die Grundsätze und Maßnahmen zu einem bestimmten Zeitpunkt implementiert waren. Die Wirksamkeitsprüfung stellt die abschließende Stufe dar und befasst sich damit, ob die Prüfungssubjekte der ersten und zweiten Stufe während eines bestimmten Zeitraums wirksam waren.

Wenngleich der eher kaufmännisch ausgerichtete Prüfungsstandard einen einheitlichen Maßstab für CMS festlegt und erstmalig eine Prüfung dieser erlaubt, können vereinzelte Anforderungen des IDW PS 980 von den Prüfenden je nach Unternehmen, Größe, Bedarf und Risikolage unterschiedlich interpretiert werden. Allerdings fehlt es dem PS 980 an Anerkennung im internationalen Geschäftsverkehr, wenngleich dieser ebenso wie alle anderen IDW-Prüfungsstandards den International Standards on Auditing (ISA) unter Berücksichtigung von Anpassungen an geltendes deutsches Recht entsprechen.

Die ISO-Zertifizierung als internationaler Standard

2014 erschien mit der DIN ISO 19600 ein sog. B-Standard, der international Wirkung beim Aufbau eines CMS erzielte und ein Best-Practice darstellt, der allerdings als nicht prüfbarer Standard nicht den IDW PS 980 ersetzen konnte. Bei der ISO 19600 handelt es sich somit mehr um eine internationale Guideline als einen prüfbaren Anforderungskatalog an ein wirksames CMS.

Mit der jüngst verabschiedeten internationalen Norm ISO 37301:2021 wird nun erstmals eine echte Alternative zum IDW PS 980 diskutiert, da diese im Vergleich zu ihrer Vorgängerin, der ISO 19600 über Empfehlungen hinaus auch konkrete Anforderungen enthält, akkreditierungsfähig ist und entsprechend zertifiziert werden kann. Eine CMS-Implementierung nach ISO 37301 kann nicht nur die Entwicklung und Verbreitung einer positiven Compliance-Kultur fördern, sondern ermöglicht darüber hinaus auch die Konformitätsbewertung und anschließende Zertifizierung eines unabhängigen Dritten.

Aufbau der ISO 37301

Im Aufbau ähnelt die ISO 37301 den Zertifizierungen anderer Management-Systeme, wie etwa der ISO 9001 (Qualitätsmanagement-Systeme), ISO 14001 (Umweltmanagementnorm) oder der ISO 37001 (Management-Systeme zur Korruptionsbekämpfung) und lässt sich so auch durch den Einsatz des Plan-Do-Act-Check-Zyklus (PDAC) individuell

auf die Größe und Struktur der Organisation skalieren. Auch die ISO 37301 definiert sieben zentrale Management Controls als Anforderungen für die Bemessung des Reifegrades eines (wirksamen) CMS:

- **Kontext der Organisation**
  In einem ersten Schritt geht es darum, die spezifischen Anforderungen an das unternehmensindividuelle Compliance-Management-System zu definieren und zu analysieren, um so ein allgemeines Verständnis zu schaffen. Darunter fällt im i. e. S. die Analyse des Unternehmensumfeldes unter Berücksichtigung interner sowie externer Faktoren. Ziel der Organisation sollte der Aufbau, die Verwirklichung, die Aufrechterhaltung sowie die fortlaufende Verbesserung eines Compliance-Management-Systems sein, welches die Werte, Ziele, Strategie und Compliance-Risiken im Kontext der Organisation widerspiegelt.

- **Führung**
  Wirksame Compliance gelingt nur, wenn sie die gesamte Organisation durchdringt und das oberste Organ klar und deutlich eine aktive Verpflichtung ausstrahlt (Tone from the Top). Zudem sollte die Organisation eine wirksame Compliance-Politik entwickeln, welche deren Anwendung, den Umfang und den Kontext darlegt sowie die Grundsätze definiert, auf deren Basis die Beziehungen zu internen und externen interessierten Parteien gehandhabt werden.

- **Planung**
  Die Planung des Compliance-Management-Systems erfolgt auf strategischer Ebene und dient der Antizipation möglicher Risiko-Szenarien sowie der Erarbeitung geeigneter Gegenmaßnahmen. Darüber hinaus befasst sie sich mit der Fragestellung, wie sie von günstigen Bedingungen oder Umständen profitieren kann, die die Wirksamkeit des Compliance-Management-Systems unterstützen können. Zuletzt wird im Rahmen der Planung ein CMS-Scope definiert.

- **Unterstützung**
  Ein wirksames CMS setzt neben der Bestimmung sowie Bereitstellung erforderlicher Ressourcen auch den Einsatz eines angemessenen Kompetenz- und Informationsmanagements voraus. Zudem muss die Organisation die interne sowie externe Kommunikation abstimmen und insb. bei den Personen, die entsprechende Tätigkeiten verrichten, ein Bewusstsein für das Compliance-Thema schaffen.

- **Betrieb**
  Ein gut gestaltetes Compliance-Management-System umfasst Maßnahmen (z. B. Richtlinien, Prozesse, Verfahren), die einer Compliance-Kultur Inhalt und Wirkung verleihen. Sie greifen die im Prozess identifizierten Compliance-Risiken auf und zielen auf deren Reduzierung ab.

- **Bewertung der Leistung**
  Um sicherzustellen, dass die Ziele erreicht werden, stellt die Bewertung des Compliance-Management-Systems sowie deren vorangegangene Überwachung, Messung, und Analyse ein wirksames Werkzeug dar. Dazu zählt etwa auch die regelmäßige Durchführung interner Audits. Die Geschäftsführung bzw. der Compliance-Verantwortliche müssen das Compliance-Management-System der Organisation in laufenden Abständen bewerten, um dessen fortdauernde Eignung, Angemessenheit und Wirksamkeit sicherzustellen.

- **Verbesserung**
  Die fortlaufende Verbesserung eines Compliance-Management-Systems stellt nach der ISO 37301 eine zentrale Anforderung dar. Dafür muss die Organisation bei Nichtkonformität oder Non-Compliance angemessen reagieren, die getroffenen Maßnahmen zur Vermeidung dieser bewerten und anschließend jegliche erforderliche Maßnahme einleiten. Die wiederkehrende Überprüfung und ggf. Vornahme von Korrekturmaßnahmen an einem bestehenden Compliance-Management-System sind feste Bestandteile einer fortlaufenden Verbesserung.

Zertifizierung von Management-Systemen

Umfassende Regulatorik, der Gesetzgeber Nachhaltigkeitsthemen und Corporate Social Responsibility, Wettbewerber, Kunden und Lieferanten, aber auch das eigene Risikobewusstsein führen dazu, dass sich Unternehmen verstärkt den umfassenden Anforderungen an ein Compliance-Management-System stellen müssen. Die Anforderungen all dieser Stakeholder in einem ganzheitlichen Compliance-Management-System umzusetzen, bringt enorme Vorteile mit sich. Die Ziele einer Zertifizierung von Management-Systemen sind bereichsübergreifend vergleichbar und können allgemein unter der Optimierung interner Prozesse, der Minimierung von Risiken und der systematischen Erfüllung von Kundenerwartungen zusammengefasst werden. Nicht zuletzt um die Akzeptanz auf nationaler und internationaler Ebene sowie im Welthandel zu fördern, können sich Zertifizierungsstellen auf der normativen Grundlage der internationalen Norm ISO/IEC 17021 durch die Deutsche Akkreditierungsstelle (DakkS) akkreditieren lassen.

Ansprechpartner

Als Ansprechpartnerin für Ihre Fragen im Bereich der Implementierung von Compliance-Management-Systemen steht Ihnen Sabine Riederer, Zert. Datenschutzbeauftragte (GDD), CDPSE, ISO 27001 LA, Senior Managerin bei Ebner Stolz in München zur Verfügung.

Bestätigung der ISO 9001

Management-Systeme unterstützen Organisationen dabei, ihre Aufgaben planvoll anzugehen und ihre gesteckten Ziele zu erreichen – durch klare Strukturen und festgelegte Prozesse. Diese Vorgehensweise hilft, interne Abläufe zu optimieren, Risiken zu minimieren oder Kundenerwartungen systematischer zu erfüllen. Zu den Management-Systemen gehört auch die ISO 9001 – Qualitätsmanagement-Systeme. Bei dieser Norm handelt es sich um die am meisten zertifizierte Norm in Deutschland.

DIN-Normen werden spätestens alle fünf Jahre dahingehend überprüft, ob sie weiterhin aktuell sind. Wird festgestellt, dass diese nicht mehr dem aktuellen Stand der Technik entsprechen, werden sie überarbeitet – siehe bspw. dazu auch die Überarbeitung der ISO 27002. Eine Überarbeitung dauert in der Regel zwei Jahre, so dass man in einem Sieben-Jahresrhythmus ist. Die aktuelle ISO 9001 ist aus 2015, so dass eine zeitnahe Überarbeitung angestanden hätte.

Jedoch wurde die ISO 9001:2015 in diesem Jahr durch das technische Komitee ISO/TC 176/SC 2 „Strategic Planning and Operations Task Group“ (SPOTG) in Abstimmung mit den Mitgliedsorganisationen unverändert bestätigt. Eine Überarbeitung erfolgte somit nicht. Allerdings wurde festgelegt, dass geprüft werden müsse, ob mit der nächsten Revision früher als im zuvor beschriebenen Regelfall begonnen werden soll. Dies bedeutet, dass sich Unternehmen mit einer bestehenden ISO 9001-Zertifizierung zunächst einmal auf keine Änderungen einstellen müssen.

Exkurs Zertifizierung

DIN / ISO Normen wie die ISO 9001 oder die ISO/IEC 27001 finden in den unterschiedlichsten Bereichen Anwendung – bspw. Informationssicherheit, Medizintechnik, Prüflabore, Qualitätsmanagement, Energiemanagement. Für die unterschiedlichsten Normen gelten somit – rein inhaltlich – auch die verschiedensten Anforderungen. Manche Normen – wie bspw. ISO 9001 und ISO/IEC 27001 – haben einen sehr ähnlichen Aufbau, weshalb sich diese zu den Management-Systemen gezählt werden. Somit dürfen dies entsprechend ausschließlich Zertifizierungsstellen auditieren bzw. zertifizieren, welche für die Norm DIN EN ISO/IEC 17021-1 (Zertifizierung von Management-Systemen) bei der Deutschen Akkreditierungsstelle (DAKkS) akkreditiert sind. Diese Norm legt fest, welche allgemeinen sowie speziellen Anforderungen diese Zertifizierungsstellen im Hinblick auf Unabhängigkeit, Struktur, Ressourcen und Prozesse erfüllen muss, um als kompetent und unparteilich eingestuft zu werden.

Anhand des Beispiels der IOS/IEC 27701 (Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management von Informationen zum Datenschutz) zeigt sich, worauf im Rahmen dessen zu achten ist. Gemäß Art. 42 DSGVO sind prinzipiell Zertifizierungen möglich, allerdings existiert durch die strengen Vorgaben der Anforderungen an die Zertifizierungsstelle gemäß Art. 43 DSGVO ein formales Problem. Art. 43 DSGVO fordert die Akkreditierung von Zertifizierungsstellen nach der DIN EN ISO/IEC17065:2013-01-Norm, welche die Anforderungen für die Zertifizierung von Produkten und Prozessen definiert. Da die ISO 27000er-Reihe sich nach den Anforderungen der DIN EN ISO/IEC 17021-1 richtet, welche auf Management-Systeme ausgerichtet ist, stellt die DIN EN ISO/IEC 27701:2019-08 keine anwendbare Zertifizierung zur Erfüllung der DSGVO dar. Eine Änderung, so dass die 27701 angewendet werden kann, ist nicht zu erwarten.

ANSPRECHPARTNER

HAMBURG

Holger Klindtworth
Tel. +49 40 37097-220
Holger.Klindtworth@ebnerstolz.de

Claudia Stange-Gathmann
CISA, CIA, CISM, QA (DIIR),
ISO/IEC 27001 LA
Tel. +49 40 37097-313
Claudia.Stange@ebnerstolz.de

DÜSSELDORF / KÖLN

Christian Wieder
CISA, CRISC
Tel.: +49 211 30143213
Christian.Wieder@ebnerstolz.de

FRANKFURT

Sebastian Adam
CISA, ISO/IEC 27001 LI
Tel. +49 69 1539249-21
Sebastian.Adam@ebnerstolz.de

MÜNCHEN

Mark Alexander Butzke
Wirtschaftsprüfer, Steuerberater, CISA, CRISC,
ISO/IEC 27001 Senior LA
Tel. +49 89 549018-292
Mark.Butzke@ebnerstolz.de

Michael Burkhardt
CISA, CRISC, ISO/IEC 27001 LA
Tel. +49 89 549018-293
Michael.Burkhardt@ebnerstolz.de

STUTTGART

Ralf Körber
Wirtschaftsprüfer, Steuerberater, CISA, CRISC
Tel. +49 711 2049-1378
Ralf.Koerber@ebnerstolz.de

John Hoffmann
CISA, CIA
Tel. +49 711 2049-1219
John.Hoffmann@ebnerstolz.de

ESECURITY-CERT GMBH

Marc Alexander Luge
ISO ISO/IEC 27001 LA,
zus. Prüfverfahrenskompetenz für § 8a (3)
BISG, IT-Sicherheitskatalog § 11 (1a und 1b)
EnWG
Tel. +49 211 540148-02
Marc.Luge@esecurity-cert.com

IMPRESSUM

Herausgeber:
Ebner Stolz GmbH & Co. KG
www.ebnerstolz.de

Ludwig-Erhard-Straße 1, 20459 Hamburg
Tel. +49 40 37097-0

Holzmarkt 1, 50676 Köln
Tel. +49 221 20643-0

Kronenstraße 30, 70174 Stuttgart
Tel. +49 711 2049-0

Redaktion:
Marc Alexander Luge, Tel. +49 211 91332-663
Hanna Pentzek, Tel. +49 211 91332-664
Dr. Ulrike Höreth, Tel. +49 711 2049-1371
novus.it@ebnerstolz.de

Wir legen großen Wert auf Gleichbehandlung. Aus Gründen der besseren Lesbarkeit verzichten wir jedoch auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers. Im Sinne der Gleichbehandlung gelten entsprechende Begriffe grundsätzlich für alle Geschlechter. Die verkürzte Sprachform beinhaltet also keine Wertung, sondern hat lediglich redaktionelle Gründe.

Fotonachweis:
©www.gettyimages.com