Fachlich-technische Normen & der Stand der Technik im Compliance Management

erstellt von

Ziviltechniker und Gerichts-SV

DDipl.-Ing. Mag. Gernot Schmied

Wien, am 14. Oktober 2022

Ziviltechniker Gernot Schmied, DDipl.-Ing. Mag.rer.soc.oec.
Marchfeldstrasse 9/41, 1200 Vienna, Austria
+43 699 19235834 . buero@gernotschmied.at
www.gernotschmied.at . Austrian Anadi Bank, SWIFT BIC: HAABAT2K
IBAN: AT27 5200 0000 0030 8161 . UID: ATU56926205

Inhalt

1. Analyse und Beschreibung der Ausgangssituation

1.1. Compliance und fachlich-technische Normen

Das Compliance Management ist intrinsisch vorausschauender und vorsorgender Natur und umfasst die Einhaltung rechtlicher und regulatorischer Normen, interner Vorgaben (Policies), Verhaltenscodizes zu Kultur und Werten, sonstige Regeln sowie **fachlich-technischer Normen** ieS („*Standards*“ in englischer Diktion). Diese Arbeit widmet sich letzterem Aspekt. Damit sind ausdrücklich nicht Normen gemeint, die die Gestaltung und Umsetzung eines CMS[1] oder IKS[2] per se regeln, diese werden bewusst ausgeklammert (ISO 37301, ISO 37001 u.a).

Solche fachlich-technische Normen betreffen in unterschiedlicher Form jede Branche in sehr spezifischer Form. Bedingt durch die Fortschritte und Durchdringung der Informationstechnologie und Automatisierung gibt es darüber hinaus Normen, Standards und good Practices, die wohl branchenübergreifend von allgemeiner Bedeutung sind. Befasst man sich mit rechtlich-regulatorischen Themengebieten, erkennt man auch darin eine intrinsische Überlappung mit fachlich-technischen Normen.

Grundsätzlich kann jedoch nicht davon ausgegangen werden, dass sich das Compliance Management dafür zuständig erachtet oder es ausreichendes Bewusstsein für Normeneinschätzung, -beobachtung und -lenkung als integralen Bestandteil der Harmonisierungs- und Supervisionsaufgaben gibt.

Offen bleibt ebenfalls, ob die Befassung strukturiert und als kontinuierlicher iterativer Prozess erfolgt und durch wen, sowie zentralisiert oder als verteilter Ansatz innerhalb der Aufbau- (Technik, Produkt- oder Projektmanagement) und Ablauforganisation. Ergänzend, ob sich CMS- und GRC[3]-Lösungen auch dafür eignen. Ausreichende Normenbefassung und Nachweise dafür sind jedenfalls auch ein klassisches Dokumentenlenkungs- und Change-Tracking-Thema.

Erschwerend kommt hinzu, dass in den meisten Branchen von komplexen und vielfältigen Normengebilden auszugehen ist, die je nach Innovationsgrad erheblich hinter der Branchenrealität nachhinken können. Auch darf nicht unterschätzt werden, dass Normen ggf. mitverbindliche ergänzende Normen referenzieren können und dadurch erheblicher Aufwand und Komplexität entstehen kann. Auch die Revisionsdynamik von Normen stellt sich unterschiedlich dar, dazugehöriges Release-Management nebst ggf. Übergangsfristen ist ebenfalls aufwändig.

1.2. Compliance und der Begriff „lege artis“

Man spricht in diesem Zusammenhang von einer fachgerechten Ausführung/Handlung „*lege artis*“ (nach den Regeln der Kunst).

Lege artis („nach den Regeln der Kunst“, von lateinisch lex, legis, „Gesetz“ und lateinisch ars, artis, „Kunst“; englisch „State of the Art“) ist im Haftungsrecht der Rechtsgrundsatz, wonach eine vertragliche Leistungspflicht entsprechend dem Stand der Wissenschaft, den anerkannten Regeln der Technik, den gesellschaftlichen Normen oder den Rechtsnormen sowie unter Einsatz der körperlichen und geistigen Fähigkeiten, Fertigkeiten und Kenntnisse zu erfüllen ist.[4]

[1] Compliance Management System
[2] Internes Kontroll-System
[3] Governance, Risk and Compliance
[4] https://de.wikipedia.org/wiki/Lege_artis

Dem widersprechend vertrete ich die Ansicht, dass mit „*state oft he art*“ in moderner Auslegung dieses englischen Idioms mehr der Stand der Technik eines Verfahrens, Produktes oder einer Technologie gemeint ist und nicht eine wörtliche Übersetzung von „*lege artis*“, die sich essenziell auch auf Fertigkeiten, Kompetenzen und Fähigkeiten *ad personam* bezieht.

Eine Ausführung, die nicht *lege artis* erfolgt, ist im Umkehrschluss potenziell mangelhaft, dabei ist insbesondere der besondere Sorgfaltsmaßstab von Sachverständigen und besonderen freien Berufen nach ABGB §1299[5] zu berücksichtigen.

1.3. Compliance und Konformität: Normenanwendung und -umsetzung

Bei der Frage der Einhaltung rechtlicher und gesellschaftlicher Normen ist der Begriff „Compliance“ intuitiv und etabliert. „*To comply*“ bedeutet entsprechen, befolgen oder erfüllen. Geht es allerdings um die Frage fachlich-technischer Normen und deren Anwendungs-, Umsetzungs- und Abdeckungsgrad, so ist der Begriff „Konformität“ zweckmäßiger.

Werden fachlich-technische Normen explizit *ex lege* für verbindlich erklärt oder direkt als Nachweis für Compliance referenziert, resultiert daraus eine im Zweifel vollumfängliche Verpflichtung zur Konformität. Darüber hinaus ist es eine dispositive Ermessensfrage, ob man fachlich-technische Normen überhaupt heranzieht, in welchem Ausmaß oder sich daran lose oder auch nur auszugsweise orientiert. Letztendlich ist diese Entscheidung auch davon abhängig, ob eine mögliche Zertifizierung angestrebt wird und die spezifische Norm überhaupt zertifizierbar bzw. akkreditierbar ist.

Ebenfalls dispositiv ist die Wahl eines ggf. vorhandeneren Umsetzungsframeworks wie z.B. für das Risikomanagement, COBIT, COSO, ITIL u.a. Damit verbunden kann der Begriff „SOA“ (*Statement of Applicability*) aus dem Bereich der Managementsystemnormen als Ergebnis einer Relevanzbetrachtung für die Organisation und deren Branchenkontext gute Dienste leisten, um zu begründen, warum Normen nur teilumfänglich oder gar nicht beachtet wurden.

Die Anwendung fachlicher Normen erfüllt u.a. die folgenden Zwecke:

- Einhaltung expliziter rechtlicher oder regulatorischer Vorgaben, Transparenz
- Beleg für *due diligence* (hinreichende Sorgfalt und Umsicht) hinsichtlich der Anwendung des Standes der Technik oder eine Ausführung *lege artis*
- Markt- bzw. Zertifizierungsdruck begegnen, Wettbewerbsfähigkeit erhalten
- Faktische Unumgänglichkeit für das Kerngeschäft (Branchen-Gepflogenheit, Usance, Verkehrssitte) → „*conditio sine qua non*“
- Innovationsmanagement

Unter Umsetzung oder Anwendung ist sehr oft die Einrichtung von Vorkehrungen (präventiven und detektiven bzw. monitoring Controls) sowie reaktiven Maßnahmen zu verstehen. Dabei stellt sich die

[5] Wer sich zu einem Amte, zu einer Kunst, zu einem Gewerbe oder Handwerke öffentlich bekennet; oder wer ohne Noth freywillig ein Geschäft übernimmt, dessen Ausführung eigene Kunstkenntnisse, oder einen nicht gewöhnlichen Fleiß erfordert, gibt dadurch zu erkennen, daß er sich den nothwendigen Fleiß und die erforderlichen, nicht gewöhnlichen Kenntnisse zutraue; er muß daher den Mangel derselben vertreten. Hat aber derjenige, welcher ihm das Geschäft überließ, die Unerfahrenheit desselben gewußt; oder, bey gewöhnlicher Aufmerksamkeit wissen können; so fällt zugleich dem Letzteren ein Versehen zur Last.

Frage aus anderer Perspektive, ob denn eine etablierte Control oder getroffene Maßnahme dem Stand der Technik hinreichend genügt und dieser Umstand plausibel belegt werden kann, die Normkonformität in gelebter Praxis somit belegt werden kann.

1.4. Compliance und der „Stand der Technik“

Für den „*Stand der Technik*“ gibt es keine allgemein gültigen und lediglich wenig spezifischen Legaldefinitionen, obwohl im rechtlichen Kontext geradezu „inflationär“ verwendet. Dies liegt wohl darin begründet, dass es erheblich auf den Kontext ankommt und sich der „*Stand der Technik*“ in ständigen Fluss befindet, ebenso Normengruppen. Auch aus dem Konsens verschiedener Sachverständigenmeinungen alleine resultiert keine vollständig gesicherte Aussage dazu.

Von geringer praktischer Relevanz ist a priori der *Stand der Wissenschaft*, da eher ein Gradmesser für Innovation, die eine bestimmte Branche noch nicht maßgeblich durchdrungen hat, Umsetzungen verfügbar sind bzw. eine nennenswerte Verbreitung erfahren hat. Es gibt jedoch Branchen, wo diese beiden Kategorien sehr nahe beieinander liegen, denken wir beispielsweise an Pharmazie oder Medizin sowie Kryptographie. Die Verknüpfung „*des Standes der Technik und der Wissenschaft*“ kommt zuweilen ebenfalls vor, diese Formulierung findet sich in rechtlichen Materien jedoch wesentlich seltener und erhöht die Unsicherheit in der Auslegung.

Fachlich-technische Normen werden in rechtlicher Diskussion idR. als wenig reflektierter und oftmals einziger Maßstab für den Stand der Technik allgemein und pauschal angeführt. Dies unbeachtet des trägen und mitunter defizitären Normungsprozesses, der keineswegs frei von Realitätsferne, Qualitätsmängeln, Lobbying und Interessenkonflikten ist und oftmals schlechte Kompromisse abbildet, die selbst innerhalb der mitgestaltenden Branchen unmöglich vollumfänglich umgesetzt werden können, schon gar nicht in historisch gewachsenen Strukturen mit damit verbunden Sachzwängen. Eine Sachverständigenbefassung damit hat jedenfalls ganzheitliche zu erfolgen.

Die Frage der Beurteilung von Aktualität, Qualität, Tauglichkeit und Relevanz von Normen ist daher von zentraler Bedeutung, als wesentliche Kriterien sind die Akzeptanz und nachweislich gelebte Anwendung innerhalb einer Branche maßgeblich. Rechtsnormen wie z.B. das DSG gestattet ferner eine Verhältnismäßigkeitsbetrachtung hinsichtlich der wirtschaftlichen Zumutbarkeit. Abbildung 1 ist daher immer auf den **Kontext einer spezifischen Branche und Geschäftstätigkeit** anzuwenden. Der „*Stand der Technik*“ ist von „*allgemein anerkannten Regeln der Technik*“ wohl nicht exakt abgrenzbar, in der Anwendungspraxis rate ich, beide Aspekte gesamtheitlich zu behandeln.

WEKA[6] meint dazu in Anlehnung an das bundesdeutsche „Handbuch der Rechtsförmlichkeit“ vom 22. September 2008:

*Dem Stand der Technik entspricht die im europäischen Recht oft verwendete Formulierung „**die besten verfügbaren Techniken**”. Dies bringt sehr deutlich einen Unterschied zum Stand von Wissenschaft zum Ausdruck: Die dem Stand der Technik entsprechenden Verfahren, Einrichtungen und Betriebsweisen müssen auf dem Markt verfügbar sein. Das sind sie aber nur, wenn ein Bedarf danach besteht, wenn also*

- *die führenden Fachleute die Verfahren, Einrichtungen und Betriebsweisen für geeignet halten, das jeweils angestrebte Schutzziel zu erreichen,*

[6] https://www.weka.de/produktsicherheit/stand-der-technik-3/

- *die Verfahren, Einrichtungen und Betriebsweisen sich in der Praxis – im Betrieb – bewährt haben und schließlich*
- *die Verfahren, Einrichtungen und Betriebsweisen wirtschaftlich sind, ihr Einsatz also auch finanziell vertretbar oder sogar attraktiv ist.*

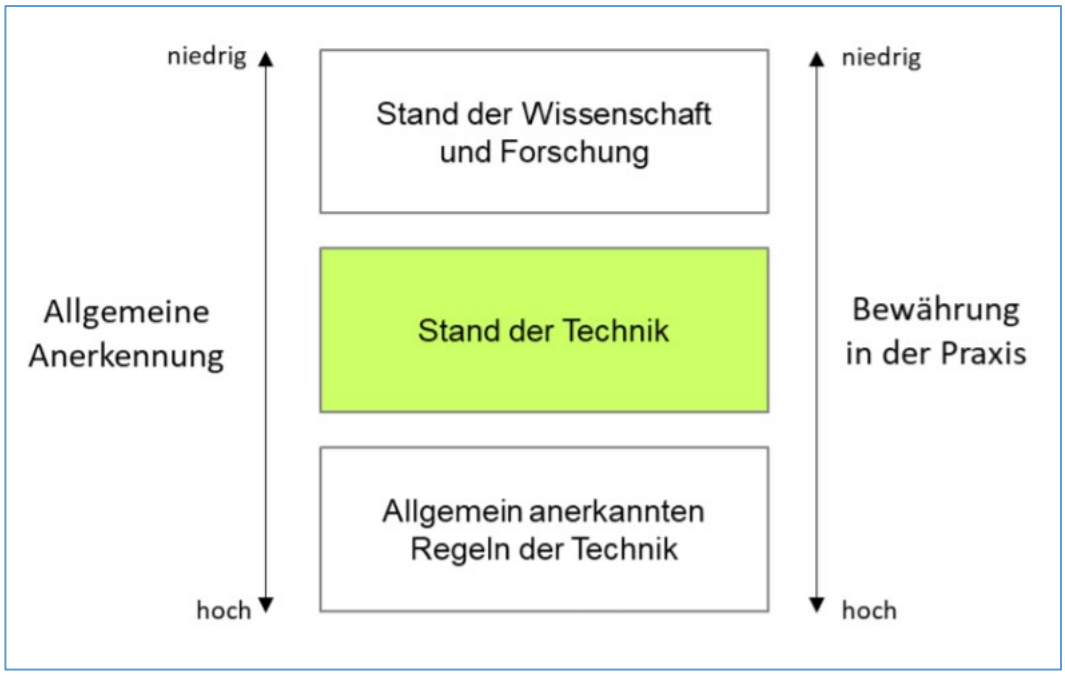


Abbildung 1 Kategorisierung nach "Handreichung zum "Stand der Technik"[7]

1.5. Ausgewählte Funde zu Legaldefinitionen „Stand der Technik“

- Gemäß Artikel 3 Nr. 10 der EU-Industrieemissionsrichtlinie (**Richtlinie 2010/75/EU**) bezeichnet der Ausdruck „**beste verfügbare Techniken**“
    - „den effizientesten und fortschrittlichsten Entwicklungsstand der Tätigkeiten und entsprechenden Betriebsmethoden, der spezielle Techniken als praktisch geeignet erscheinen lässt, grundsätzlich als Grundlage für die Emissionsgrenzwerte zu dienen, um Emissionen in und Auswirkungen auf die gesamte Umwelt allgemein zu vermeiden oder, wenn dies nicht möglich ist, zu vermindern;
    - ‚Techniken‘ sowohl die angewandte Technologie als auch die Art und Weise, wie die Anlage geplant, gebaut, gewartet, betrieben und stillgelegt wird;
    - ‚verfügbar‘ die Techniken, die in einem Maßstab entwickelt sind, der unter Berücksichtigung des Kosten/Nutzen-Verhältnisses die Anwendung unter in dem betreffenden industriellen Sektor wirtschaftlich und technisch vertretbaren

[7] https://www.teletrust.de/publikationen/broschueren/stand-der-technik/

Verhältnissen ermöglicht, gleich, ob diese Techniken innerhalb des betreffenden Mitgliedstaats verwendet oder hergestellt werden, sofern sie zu vertretbaren Bedingungen für den Betreiber zugänglich sind;

- ‚beste' die Techniken, die am wirksamsten zur Erreichung eines allgemein hohen Schutzniveaus für die Umwelt insgesamt sind."

Die Definition von „**beste verfügbare Techniken**" erfordert eine Entwicklung der Technik in einem Maßstab, der eine branchenspezifische Umsetzung ermöglicht.

- Eine allgemeine Beschreibung des Begriffs „*Stand der Technik*" findet sich im „**Handbuch der Rechtsförmlichkeit**" des Bundesjustizministeriums der Justiz (DE) vom September 2008:

  Stand der Technik ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, der nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlich vorgegebenen Zieles gesichert erscheinen lässt. Verfahren, Einrichtungen und Betriebsweisen oder vergleichbare Verfahren, Einrichtungen und Betriebsweisen müssen sich in der Praxis bewährt haben oder sollten – wenn dies noch nicht der Fall ist – möglichst im Betrieb mit Erfolg erprobt worden sein.

- **GewO: § 71a.**

  (1) Der *Stand der Technik* (**beste verfügbare Techniken – BVT**) im Sinne dieses Bundesgesetzes ist der auf den einschlägigen wissenschaftlichen Erkenntnissen beruhende Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen, Bau- oder Betriebsweisen, deren Funktionstüchtigkeit erprobt und erwiesen ist. Bei der Bestimmung des Standes der Technik sind insbesondere jene vergleichbaren Verfahren, Einrichtungen Bau- oder Betriebsweisen heranzuziehen, welche am wirksamsten zur Erreichung eines allgemein hohen Schutzniveaus für die Umwelt insgesamt sind; weiters sind unter Beachtung der sich aus einer bestimmten Maßnahme ergebenden Kosten und ihres Nutzens und des Grundsatzes der Vorsorge und der Vorbeugung im Allgemeinen wie auch im Einzelfall die Kriterien der Anlage 6 zu diesem Bundesgesetz zu berücksichtigen.

  (2) Für Wasserbenutzungen, Maßnahmen, Einwirkungen und Anlagen, für die der Stand der Technik nach dem WRG 1959 festgelegt ist oder wird, ist dieser maßgebend.

  (3) Für Anlagen, in denen Abfälle behandelt werden, für die der Stand der Technik nach dem AWG festgelegt ist oder wird, ist dieser maßgebend.

- **BVergG:** Mit der Novelle des BVergG 2018 wurde eine als „Normenbindung" bzw. „Normenbezug" bekannte generische Besonderheit im Umgang mit vertraglichen und fachlich-technischen Normen stark gelockert. Davor waren „*bei der Erstellung eines Leistungsverzeichnisses geeignete Leitlinien, wie ÖNORMEN oder standardisierte Leistungsbeschreibungen heranzuziehen*" [8], nach dem BVergG 2018 ist auf diese nur mehr „*Bedacht zu nehmen*" (§ 105 Abs. 3 und § 110 Abs. 2).

[8] ZVB Februar 2009 – „Der Bezug auf technische Normen im BVergG – unbeachtete Facetten aus fachlichem Blickwinkel", Gernot Schmied

1.1. Beispiele für den Bezug auf den „Stand der Technik“ in österreichischen IT-Rechtsnormen

- TKG (2003) § 16a.

  (1) Betreiber öffentlicher Kommunikationsnetze haben geeignete Maßnahmen zur Gewährleistung der Integrität ihrer Netze zu ergreifen und die fortlaufende Verfügbarkeit der über diese Netze erbrachten Dienste sicher zu stellen.

  (2) Betreiber öffentlicher Kommunikationsnetze oder -dienste haben unter Berücksichtigung des *Standes der Technik* durch angemessene technische und organisatorische Maßnahmen ein Sicherheitsniveau zu gewährleisten, das zur Beherrschung der Risiken für die Netzsicherheit geeignet ist. Die Maßnahmen müssen insbesondere geeignet sein, Auswirkungen von Sicherheitsverletzungen für Nutzer und zusammengeschaltete Netze zu vermeiden bzw. so gering wie möglich zu halten.

- NISG § 17. (1) Zur Gewährleistung der NIS haben Betreiber wesentlicher Dienste in Hinblick auf die Netz- und Informationssysteme, die sie für die Bereitstellung des wesentlichen Dienstes nutzen, geeignete und verhältnismäßige *technische und organisatorische Sicherheitsvorkehrungen* zu treffen. Diese haben den *Stand der Technik* zu berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein.

  NISG § 21. (1) Zur Gewährleistung der NIS haben Anbieter digitaler Dienste in Hinblick auf die Netz- und Informationssysteme, die sie für die Bereitstellung des digitalen Dienstes nutzen, geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen. Diese haben unter Berücksichtigung des *Stands der Technik* ein Sicherheitsniveau der Netz- und Informationssysteme zu gewährleisten, dass dem bestehenden mit vernünftigem Aufwand feststellbaren Risiko angemessen ist, wobei Folgendem Rechnung getragen wird:

  a) Sicherheit der Systeme und Anlagen,

  b) Bewältigung von Sicherheitsvorfällen,

  c) Betriebskontinuitätsmanagement,

  d) Überwachung, Überprüfung und Erprobung,

  e) *Einhaltung der internationalen Normen*.

- NISV § 11. (1) Sicherheitsvorkehrungen gemäß § 17 Abs. 1 NISG, die geeignet sind und den *Stand der Technik* berücksichtigen sowie zur Gewährleistung der Netz- und Informationssystemsicherheit (§ 3 Z 2 NISG) zu treffen sind, umfassen die [….]

- DSG § 54. (1) Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des *Stands der Technik*, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, unter Berücksichtigung der unterschiedlichen Kategorien gemäß § 37, geeignete *technische und organisatorische Maßnahmen* zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß § 39.

- MPG (Medizinproduktegesetz)

  MPG § 11. (2) Medizinprodukte für die in-vitro-Diagnose müssen so ausgelegt und hergestellt sein, dass sie unter Berücksichtigung des *allgemein anerkannten Standes der Technik* für die vom Hersteller festgelegte Zweckbestimmung gemäß § 2 Abs. 5 geeignet sind.

  MPG §73. (8) Der Geschäftsführer der Gesundheit Österreich GmbH hat sicherzustellen, dass Identität und Rolle der Zugriffsberechtigten bei jedem Zugriff dem *Stand der Technik* entsprechend nachgewiesen und protokolliert werden. Er muss sicherstellen, dass geeignete, dem jeweiligen *Stand der Technik* entsprechende Vorkehrungen getroffen werden, um eine Vernichtung oder Veränderung der Daten durch Programmstörungen (Viren) zu verhindern, um eine Vernichtung, Veränderung oder Abfrage der Daten des Registers durch unberechtigte Benutzer oder Systeme zu verhindern. Weiters muss er sicherstellen, dass alle durchgeführten Verarbeitungsvorgänge, wie insbesondere Eintragungen, Änderungen, Abfragen und Übermittlungen, nachvollziehbar sind. Er hat ein Datensicherheitskonzept zu erstellen, das für die Mitarbeiter der Gesundheit Österreich GmbH verbindlich ist.

- GTelG § 6. (1) Die Vertraulichkeit bei der elektronischen Übermittlung von Gesundheitsdaten und genetischen Daten ist dadurch sicherzustellen, dass entweder

  die elektronische Übermittlung von Gesundheitsdaten und genetischen Daten über Netzwerke durchgeführt wird, die entsprechend dem *Stand der Technik* in der Netzwerk-sicherheit gegenüber unbefugten Zugriffen abgesichert sind, [….]

1.2. BSI-DE & TeleTrust

Das BSI hält im Zusammenhang mit der Umsetzung des Standes der Technik fest[9] [10]:

"Stand der Technik" ist ein gängiger juristischer Begriff. Die technische Entwicklung ist schneller als die Gesetzgebung. Daher hat es sich in vielen Rechtsbereichen seit vielen Jahren bewährt, in Gesetzen auf den "Stand der Technik" abzustellen, statt zu versuchen, konkrete technische Anforderungen bereits im Gesetz festzulegen.

Was zu einem bestimmten Zeitpunkt "Stand der Technik" ist, lässt sich zum Beispiel anhand existierender nationaler oder internationaler Standards und Normen von beispielsweise DIN, ISO, DKE oder ISO/IEC oder anhand erfolgreich in der Praxis erprobter Vorbilder für den jeweiligen Bereich ermitteln. Da sich die notwendigen technischen Maßnahmen je nach konkreter Fallgestaltung unterscheiden können, ist es nicht möglich, den "Stand der Technik" allgemeingültig und abschließend zu beschreiben.

Eine in deutschsprachigen Raum umfassende Befassung stellt das Dokument „*Handreichung zum Stand der Technik*“ dar, erarbeitet vom Bundesverband IT-Sicherheit e.V/TeleTrust[11]. Dieses wird als Ausgangspunkt für Betrachtungen empfohlen, ebenso das darin erläuterte Vorgehensmodell, das in Kapitel 3.1 beschrieben wird.

[9] https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Stand-der-Technik-umsetzen/stand-der-technik-umsetzen_node.html
[10] https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/KRITIS_Hilfestellung_fuer_Pruefer_Auditierung_020720.html
[11] https://www.teletrust.de/publikationen/broschueren/stand-der-technik/

1.3. Kritik der „normativen Vernunft“

Wie bereits angedeutet, ist der Entstehungsprozess von fachlich-technischen Normen, Regeln der Technik, good Practices etc. ebenso politisch und Lobbying unterworfen, wie bei rechtlichen Normen. Es gibt gute und schlecht Normen wie auch legistische Sternstunden und „Ausrutscher“ in der Gesetzesentstehung. Diese Entwicklung erfolgt in Normungsgremien ieS., Industry Alliances, Branchenvertretungen oder auch Internet Communities.

Worin besteht nun die „Kritik der normativen Vernunft“[12]?

Normen hinken der technischen Entwicklung teilweise um mehrere Jahre nach, sind mitunter schlecht formuliert oder übersetzt, mehrdeutig oder wenig praxistauglich, reich an entbehrlichen „Füllstoffen“ ohne Substrat, zu komplex und regulierungswütig und mitunter sogar bestimmte Marktteilnehmer bevorzugend.

Lehnen sich Sachverständige an Normen an, ist immer die Relevanz für und die Akzeptanz in eine Branche und deren Qualität und Aktualität zu berücksichtigen. Die bloße Existenz irgendwelcher Normen sagt per se noch nichts darüber aus. Auch gilt es den Stufenbau der Normung zu beachten (Regeln, Entwürfe, nationale, europäische und internationale Normen) sowie die Frage der Herkunft (Normungsgremien ieS oder andere wie z.B. ISO, ITU, ETSI, IEEE, CEN, CENELEC, DIN, ÖNORM, RIPE, ICANN, IETF, W3C, WIFI-Alliance etc.).

Eine ausführliche Betrachtung der Einstufung von Gremien sprengt allerdings den Rahmen dieser Arbeit, auch die Frage, wie dabei Einrichtungen wie ENISA, BSI-DE einzuschätzen sind oder Eirichtungen im Umfeld regulatorischer Governance wie z.B. FMA/OeNB, EZB, EBA. Genau darum geht es ja in einer **strukturierten Normenbeobachtung**.

[12] In Anlehnung an Immanuel Kant

2. Awareness & Risikobetrachtung der Compliance-relevanten Problemstellungen

Ignoriert oder unterschätzt man die Relevanz fachlich-technischer Normen, können sich daraus Wettbewerbs- und Imageachteile sowie Risikoszenarien ergeben. Dbzgl. „blind spots“ sollten vermieden werden, auch ist ein Verständnis der Gemeinsamkeiten und auch Unterschiede zwischen rechtlichen und fachlich-technischen Normen wichtig.

Ein mangelnder Überblick hinsichtlich des fachlich-normativen Hintergrunds oder mangelnde Kenntnis einer Branche stellt ein breites Risikofeld dar, das von Verwaltungsstrafen über Mängeln bis zu Gefahr für Gesundheit und Leben reichen kann. Werden fachlich-technische Normen explizit *ex lege* für verbindlich erklärt oder referenziert, ergibt sich daraus eine starke direkte Verbindung in das legal Risk Management.

Entfernt man sich substanziell vom in einer Branche etablierten Stand der Technik, d.h. wie sich dbzgl. ein zumindest durchschnittlich umsichtiges Unternehmen verhalten hätte, entstehen Sorgfalts- und ggf. Fahrlässigkeitsrisiken für das Unternehmen und Verantwortliche.

Andererseits stehen dem Fragen der technischen Machbarkeit eingedenk von Rahmenbedingungen und Sachzwängen entgegen, zusätzlich die Frage der wirtschaftlichen Verhältnismäßigkeit zwischen Risiko, Aufwand und Mitigations-Nutzen. Bei ungünstigster Auslegung wird an der „**besten verfügbare Technologie**“ zur Zielerreichung gemessen, d.h. man sollte auch eine Argumentation zur Hand haben, warum dies ggf. nicht möglich ist. Ein „**best effort**“ Ansatz ist jedenfalls pragmatisch.

Lehnt man sich an die Schadenersatz-Rechtsprechung an, so ist eine Ausführung „*lege artis*“ als wesentlicher Sorgfaltsmaßstab anzusehen, insbesondere zu ärztlichen Kunstfehlern gibt es reichhaltige Rechtsprechung. Transformiert man dies in die moderne Unternehmenswelt und Compliance, geht es um Verbandshaftung und Organhaftung bei mangelnder fachlich-technischer „*due diligence*“, somit Vernachlässigung der unternehmerischen Sorgfalt und Umsicht. Es ist daher jedenfalls zu empfehlen, sich systematisch damit zu befassen, auch über den „*peace of mind*“ Ansatz von Zertifizierungen hinaus.

3. Entwicklung konkreter Compliance-Maßnahmen

3.1. Organisatorische Aspekte und Aufgabenteilung

Wer ist nun zuständig und auch kompetent für die Ersteinschätzung fachlich-technischer Normen und das damit verbundene weitere Compliance, GRC und LifeCycle Management?

Das Compliance Management sollte jedenfalls den gesamtintegrativen Überblick behalten und eigenverantwortlich wahrnehmen, verfügt aber idR. nicht über die fachlich-spezialisierte Expertise, dies selbst durchzuführen. In der Praxis werden beispielsweise Datenschutz und Managementsysteme wie ISO 9001, ISO 27001 oder ISO 20000-1 oder auch CERT gerne in eigenständige Stabstellen ausgelagert. All diese Einrichtungen bedienen sich wiederum der fachlichen Expertise technischer Abteilungen. Fachlich-technische Normen und Konformitätsbetrachtungen sind jedenfalls Bestandteil der Compliance-, Risk- und Control-Landkarte im CMS bzw. IKS und als solche zu behandeln.

Dazu gehört ebenfalls das Change-Tracking der Zeitpunkte, ab denen neue Normen anzuwenden sind oder Vorgängerversionen obsolet werden, somit eine klassische Dokumentenlenkungsaufgabe.

In der Praxis ist davon auszugehen, dass das Management von fachlich-technischen Normen ein interdisziplinäres und aufgabenteilig Unterfangen innerhalb einer Organisation darstellt. Die Bewertung und Umsetzung erfolgt idR. durch Fachabteilungen, die Zusammenführung, Erledigung und Vollständigkeitsprüfung durch das Compliance Management. Dies analog zu im Unternehmen verteilten Controls des IKS mit einem konzeptionellen harmonisierten Überbau. Normenbefassung bzw. -Awareness strahlt naturgemäß auch in das Contract Management, das Produktmanagement und den Vertrieb aus.

Wer auditiert die dbzgl. Konformität bzw. den Reifegrad der Umsetzung?

Derartige Überprüfungen können z.B. als Bestandteil regulatorischer Überwachung, Zertifizierungsvorhaben oder interner Audits erfolgen, solange sichergestellt wird, dass sich die Umsetzungsverantwortlichen nicht selbst auditieren. Grundvoraussetzung ist ein gutes Branchenverständnis und Vertrautheit mit den spezifischen Normen in Anwendung. Audits können durch das Compliance Management selbst, Stabstellen, interne Revision oder mit externer Unterstützung erfolgen.

3.2. Empfohlenes Vorgehensmodell - Prozesse & Controls (Maßnahmen, Vorkehrungen)

Es bedarf jedenfalls eines Prozesses für die Normenauseinandersetzung, der sich mit nachfolgenden Aufgaben/Prozessschritten befasst:

- Identifikation potenziell branchenrelevanter fachlich-technischer Normen (Recherche)
- Relevanz- und Akzeptanzprüfung innerhalb der Branche
- Daraus SOA ableiten
- Risikobetrachtung bei Nichtbeachtung
- Umsetzungsentscheidung und -grad
- Delta-Analysen bei Normenaktualisierung

- Harmonisierung mit Zertifizierungsprogrammen (zumeist mit Management-Review und internem Audit)
- Audits und KVP-Zyklus
- Etablierung von Controls und Quality Gates
- Maßnahmenverfolgung und Ablage von Nachweisen

Ergänzend sollte bewertet werden, ob es in Verträgen, Projektunterlagen und Angeboten erforderlich ist, Normen explizit zu referenzieren oder auch an die Organisation herangetragene Normanforderungen z.B. bei Ausschreibungen dahingehend zu beurteilen, ob relevant oder potenziell markteinschränkend. Dies erfordert weitere organisatorische Schnittstellen und übergreifende Prozesse.

3.3. Nachweise und Dokumentation

Es ist nicht davon auszugehen, dass typische Werkzeuge für das generische Compliance Management bzw. IKS vorgefertigte Templates, Controls und Workflows für jedwede branchenspezifische Normen mitbringen, bzw. nur sehr eingeschränkt. Auch gibt es keine dbzgl. automatisierten Schnittstellen in Normenverzeichnisse, sehr wohl jedoch Update Subscriptions, die bei neuen Versionen zumindest eine E-Mail versenden. Die aktive Teilnahme an der Normung, in Industrievereinigung oder Vereinen und der Besuch von Fachkonferenzen ist zu empfehlen. Dies auch deshalb, um Fehlentwicklungen, Praxisferne oder überschießender Regulierungswut früh entgegen treten zu können.

Fachlich-technische Normkonformität und Kriterien für den Stand der Technik sind als integraler Bestandteil des Compliance Management bzw. einer SWOT-Analyse zu sehen. Nachweise für die Befassung und Einschätzung sollten vorhanden sein, entweder mit den Customizing-Mitteln eines CMS oder als eigenständiges und zyklisch überarbeitetes Normen- und Maßnahmen-Tracking. Jedenfalls empfohlen wird das Verfassen einer Strategie/Policy bzgl. der Governance-Vorgaben zur Normenbehandlung und damit verbundene Awareness-Maßnahmen.

3.4. Identifikation de facto verbindlicher fachlicher Normen aus rechtlichem Kontext

Wie bereits eingangs erwähnt, sind ex lege als verbindlich referenzierte Normen oder implizit als Maßstab für Compliance beispielhaft oder taxativ aufgeführte Normen jedenfalls in das Compliance Management und die Normenbeobachtung (das Normenradar“) aufzunehmen und bilden das Bindeglied vom legal Risk/Compliance Management in die fachlich-technische Normenkonformität.

3.5. „Beurteilung des „Standes der Technik“ – Objektivierung und Systematisierung

Zu diesem Zweck wird das gut gelungenen Vorgehensmodell des Bundesverband IT-Sicherheit e.V. 2021 gemäß „Handreichung zum Stand der Technik“[13] Kapitel 2. verwiesen. Darin geht es um die

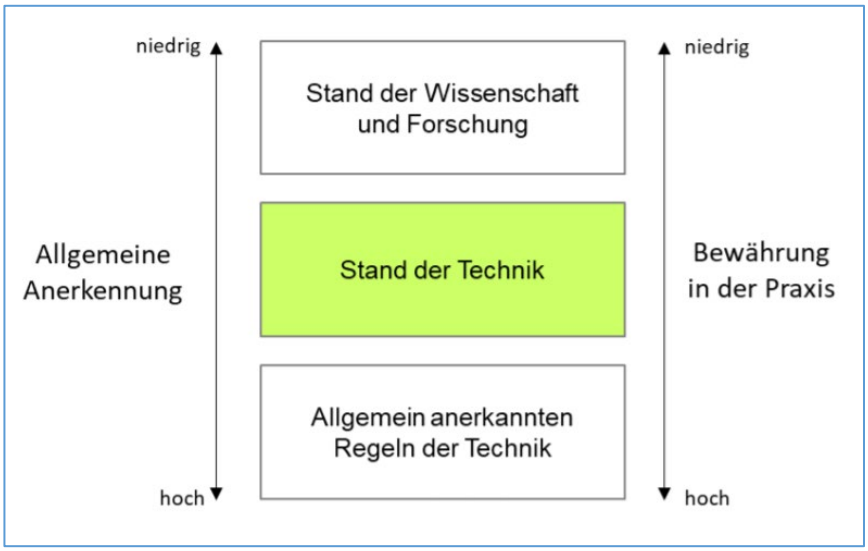
[13] https://www.teletrust.de/fileadmin/user_upload/2021-02_TeleTrusT-Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DE.pdf

Bewertung des Technologiestandes (des Standes der Technik) für technischen Maßnahmen und Controls im IT-Umfeld, eignet sich jedoch auch für branchenunabhängig-generischen Einsatz.

Ausgangspunkt der Entstehungsgeschichte[14]:

Mit dem "Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" (IT-Sicherheitsgesetz bzw. ITSiG) verfolgt der Gesetzgeber das Ziel, Defizite in der IT-Sicherheit abzubauen. Daneben gilt seit dem 25.05.2018 die EU-Datenschutz-Grundverordnung (DSGVO) mit ihren hohen Anforderungen an die technischen und organisatorischen Maßnahmen. Beide Rechtsquellen fordern die Orientierung der IT-Sicherheit am Stand der Technik, lassen aber unbeantwortet, was im Detail darunter zu verstehen ist.

Deren Vorgehensmodells zur „Bestimmung des Technologiestandes“ beruht auf der Einteilung in drei Kategorien sowie einem Katalog von Leitfragen aus dem anhand eines Punktesystems ein Mittelwert gebildet wird und dies die Positionsbestimmung ermöglicht (Abbildung 2).



1.1 Fragen zum Grad der Anerkennung — Bewertung vom Ak SdT auszufüllen.

1) Welche Dokumentation über die Maßnahme steht öffentlich zur Verfügung? *bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen*			1- w. Publikation 3- Fachmedien 5- Massenmedia
☐ wiss. Publikation	☐ Fachmedien	☐ Massenmedien	
[bitte begründen Sie Ihre Antwort hier]			
2) Nimmt die Maßnahme Bezug auf internationale oder nationale Normen? *bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen*			1- nein, noch nicht 3- ja, eine 5- ja, mehr als 1
☐ nein, noch nicht normiert	☐ ja, eine	☐ ja, mehr als eine	
[bitte begründen Sie Ihre Antwort hier]			
3) Wurde die Maßnahme von anerkannten Gremien / Verbänden empfohlen? *bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen*			1- nein 3- ja, führenden 5- ja, vielen
☐ nein	☐ ja, führenden	☐ ja, vielen	
[bitte begründen Sie Ihre Antwort hier]			
4) Wird die Eignung der Maßnahme regelmäßig überprüft? *bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen*			1- nein 3- ja, herstellerseits 5- ja, unab. Instanz
☐ nein	☐ ja, herstellerseitig	☐ ja, unabhängige Instanz	
[bitte begründen Sie Ihre Antwort hier]			
		Mittelwert	

1.2 Fragen zum Grad der Bewährung in der Praxis — Bewertung vom Ak SdT auszufüllen.

1) Wie ist der Innovationsgrad der Maßnahme einzustufen? *bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen*			1- hoch 3- mittel 5- gering
☐ hoch	☐ mittel	☐ gering	
[bitte begründen Sie Ihre Antwort hier]			
2) Wo wurde die aktuelle Version der Maßnahme erprobt? *bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen*			1- Labor 3- prof. Einsatz 5- Massenmarkt
☐ Laborbedingungen	☐ professioneller Einsatz	☐ Massenmarkt	
[bitte begründen Sie Ihre Antwort hier]			
3) Existieren vergleichbare Maßnahmen am Markt? *bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen*			1- nein 3- wenige 5- viele
☐ nein	☐ wenige	☐ viele	
[bitte begründen Sie Ihre Antwort hier]			
4) Wie oft wird die Maßnahme herstellerseitig konzeptionell aktualisiert? *bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen*			1- häuf. als 1/ Jahr 3- jährlich 5- seltener
☐ häufiger als 1/Jahr	☐ jährlich	☐ seltener	
[bitte begründen Sie Ihre Antwort hier]			
		Mittelwert	

[14] https://www.teletrust.de/publikationen/broschueren/stand-der-technik/

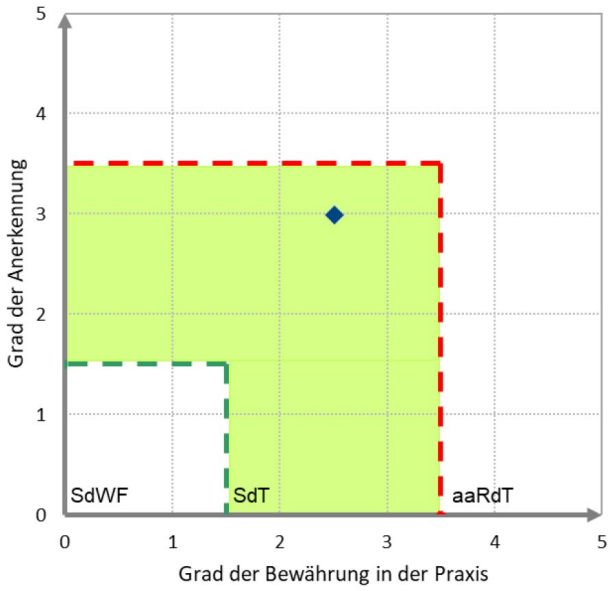


Abbildung 2 Die drei Teile zur „Bestimmung des Technologiestandes" nach "Handreichung zum "Stand der Technik"

Kritisch zu hinterfragen ist generell der Ansatz, der „Stand der Technik" beziehe sich sinngemäß auf **eine im Markt verfügbare Bestleistung** zu einer bestimmten Zielerreichung oder dem Erreichen eines Schutzziels oder der Verringerung eines Gefährdungspotenzials, das ich auch in Herangehensweise des BSI-DE[15] wiederfindet ebenso im bundesdeutschen Handbuch der Rechtsförmlichkeit und EU-Richtlinien.

Die Forderung „*the best and finest money can buy*", iSv. die besten Produkte, Architekturen, Lösungen, Controls und Spezialisten/Berater entspricht nicht mal annähernd den Branchenrealitäten, weder aus technischer, finanzieller noch Knowhow Sicht, dies nicht mal als optimalen „*greenfield approach from scratch*".

Wesentlich sinnvoller ist als durchaus rechtlich praktizierter **Vergleichsmaßstab**, wie sich ein „durchschnittlich" umsichtiges Unternehmen in einer spezifischen Branche verhalten hätte, und nicht der Klassenprimus oder eine abstrakte Organisation ohne Sachzwänge mit unbeschränkten Ressourcen. Ergo entspricht der **etablierte** „Stand der Technik" wohl eher dem Median einer Branche, insbesondere eingedenk der Möglichkeiten, historischen Altlasten und wirtschaftlichen Sachzwänge kleinere Unternehmen.

3.6. Ermittlung und Messung des Konformitätsgrades (Kennzahlen)

Dazu können zu spezifischen Normen oder ganze Normen beispielsweise Spinnennetzgrafiken zu Hauptkapiteln oder Control-Gruppen herangezogen werden, ebenso zur Identifikation von Normenbestandteilen, die auf die Organisation nicht anwendbare sind, dies kann mit einer SOA[16] kombiniert werden. Als Kennzahlen können Abdeckungsprozente oder numerische Anzahl umgesetzter Controls herangezogen werden.

[15] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/KES/kes_19-06.pdf?__blob=publicationFile&v=1
[16] Statement of Applicability

Kontrollfragen:

- Handelt es sich um eine branchen-spezifische Norm oder eine generisch branchenüber-greifende?
- Grad der Anerkennung in einer bestimmten Branche/branchenübergreifend?
- Relevanz und Bewährung in der Praxis?
- Komplexität beherrschbar? Referenzieren einer großen Zahl weiterführender oder mitgeltender Normen?

3.7. Beispiel NISG/NISV

Abbildung 3 zeigt ein Erhebungsbeispiel im Bereich der Energiewirtschaft, aus dem gut die intrinsische Verknüpfung von rechtlich-regulatorischen und fachlich-technischen Normen erkennbar ist. Dies stell einen möglichen Einstieg in die Normenbewertung dar.

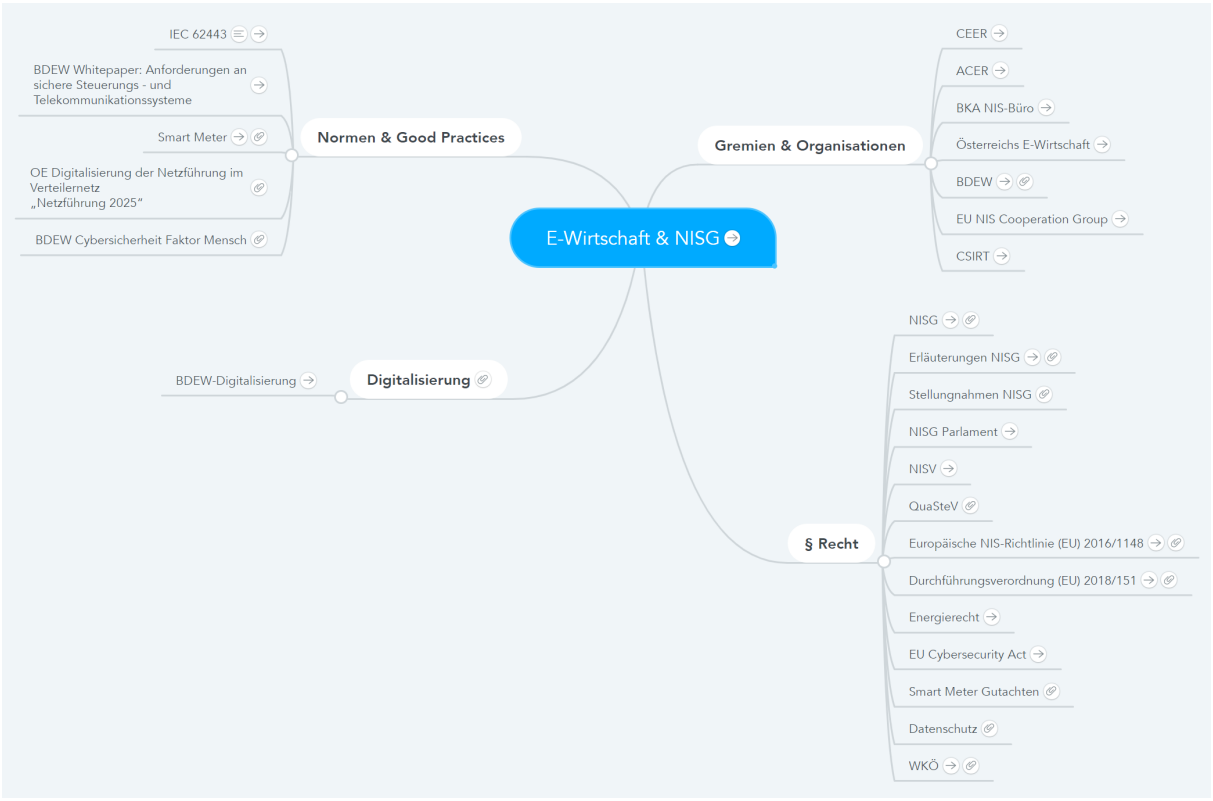


Abbildung 3 Erhebung des normativen Hintergrunds Der E-Wirtschaft und des NISG durch den Autor

4. Resümee

Die vorliegende Betrachtung dient der Bewusstseinsbildung für die Compliance-Relevanz fachlich-technischer Normen in einer bestimmten Branche im Rahmen einer spezifischen Geschäftstätigkeit und das Erfordernis einer integrierten Betrachtung und Risikoeinschätzung sowie systematischen und kontinuierlichen Herangehensweise an Normenbewertung und -beobachtung.

Maßgeblich für die Ausgangsbetrachtung ist, ob eine fachlich-technische Norm *ex lege* für verbindlich erklärt oder explizit als Maßstab für Compliance referenziert wird, sowie der Grad der Anerkennung in einer bestimmten Branche und die Relevanz und Bewährung in der Praxis in ebendieser (grundsätzliche Tauglichkeit und Praktikabilität in Umsetzung und Anwendung).

In diesem Zusammenhang wird ausführlich auf die Bedeutung des Standes der Technik und Wissenschaft, allgemeine anerkannte Regeln sowie eine Ausführung/Handlung *lege artis*, also nach den Regeln der (Branchen)Kunst, eingegangen.

Bei Unkenntnis, Nichtbeachtung oder Nichtkonformität resultieren vielfältige Risken. Werden diese schlagend, resultieren daraus zwei mögliche Einschätzungsszenarien. Entweder wird als Maßstab herangezogen, wie sich ein durchschnittlich umsichtiger Branchenteilnehmer verhalten hätte, oder im ungünstigeren Falle gemessen am Einsatz der „*besten verfügbare Technologie*“ zur Zielerreichung. Da letzter idR nicht Branchenrealitäten entspricht, wir eine pragmatische „*best effort*“ Herangehensweise als Alternative aufgezeigt, um auch einer fachlich-technischen „*due diligence*“ hinreichend zu genügen und diese zu begründen.

Ergo entspricht der **etablierte** „*Stand der Technik*“ wohl eher dem Median einer Branche, insbesondere eingedenk der Möglichkeiten, historischen Altlasten und wirtschaftlichen Sachzwänge kleinere Unternehmen und auch öffentlicher Einrichtungen.

Die Arbeit schließt mit organisatorischen und prozeduralen Empfehlungen und einem Vorschlag für die Objektivierung und Systematisierung des Technologiestandes (des Standes der Technik) für technischen Maßnahmen und Controls sowie Empfehlung für Governance, Dokumentation, Konformitätsmessung und Nachweise.

5. Quellenverzeichnis und Literatur

a. ZVB Februar 2009 – „Der Bezug auf technische Normen im BVergG – unbeachtete Facetten aus fachlichem Blickwinkel“, Gernot Schmied

b. Handbuch der Rechtsförmlichkeit BMJ-DE vom 22. September 2008, https://www.bmjv.de/DE/Themen/RechtssetzungBuerokratieabbau/HDR/HDR_node.html

c. https://www.wpno.com/stand-der-technik/

d. https://www.teletrust.de/arbeitsgremien/ak-stand-der-technik/

e. https://de.wikipedia.org/wiki/Lege_artis

f. https://de.wikipedia.org/wiki/Beste_verf%C3%BCgbare_Techniken

g. https://www.heise.de/select/ix/2017/7/1499358051209829

h. Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG V1.1 , https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/Orientierungshilfe_8a_3_v11.pdf;jsessionid=7096AEDE9C6E165E5C03FD26DB9D98BE.internet471?__blob=publicationFile&v=5

i. Lawicki, "Was bedeutet 'Stand der Technik?'", erschienen in der TeleTrusT-Sonderbeilage "Sicherheit & Datenschutz" der Zeitschrift iX 6/2018

j. Dr. Mark Seibel, Richter am OLG, https://www.dthg.de/resources/Definition-Stand-der-Technik.pdf

k. BVerfGE, 49, 89 [135 f] Kalkar-Entscheidung des Bundesverfassungsgerichts, http://de.jurispedia.org/index.php/Kalkar-Entscheidung_(de) , 08.08.1978

l. Dr. M. Seibel, Abgrenzung der „allgemein anerkannten Regeln der Technik“ vom „Stand der Technik“, Neue Juristische Wochenschrift 41/2013

m. Bartels/Backer, Die Berücksichtigung des Stands der Technik in der DSGVO, DuD 4-2018, 214; Bartels/Backer/ Schramm, Der "Stand der Technik" im IT-Sicherheitsrecht, Tagungsband zum 15. Deutschen IT-Sicherheitskongress 2017, Bundesamt für Sicherheit in der Informationstechnik, 503.

n. https://www.weka.de/produktsicherheit/stand-der-technik-3/

o. https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems.pdf

p. https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Stand-der-Technik-umsetzen/stand-der-technik-umsetzen_node.html

q. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/KES/kes_19-06.pdf?__blob=publicationFile&v=1

r. https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/KRITIS_Hilfestellung_fuer_Pruefer_Auditierung_020720.html

s. TKG 2003
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20002849

t. BVergG 2018
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010295

u. NISG
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010536

v. DSG
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597

w. MPG (Medizinproduktegesetz)
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10011003

x. GTelG 2012
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20008120

y. NISV
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010722