



Informationstag "Umsetzung des IT-Sicherheitsgesetzes in der Unternehmenspraxis"

Gemeinsame Veranstaltung von TeleTrust, bevh und BISG

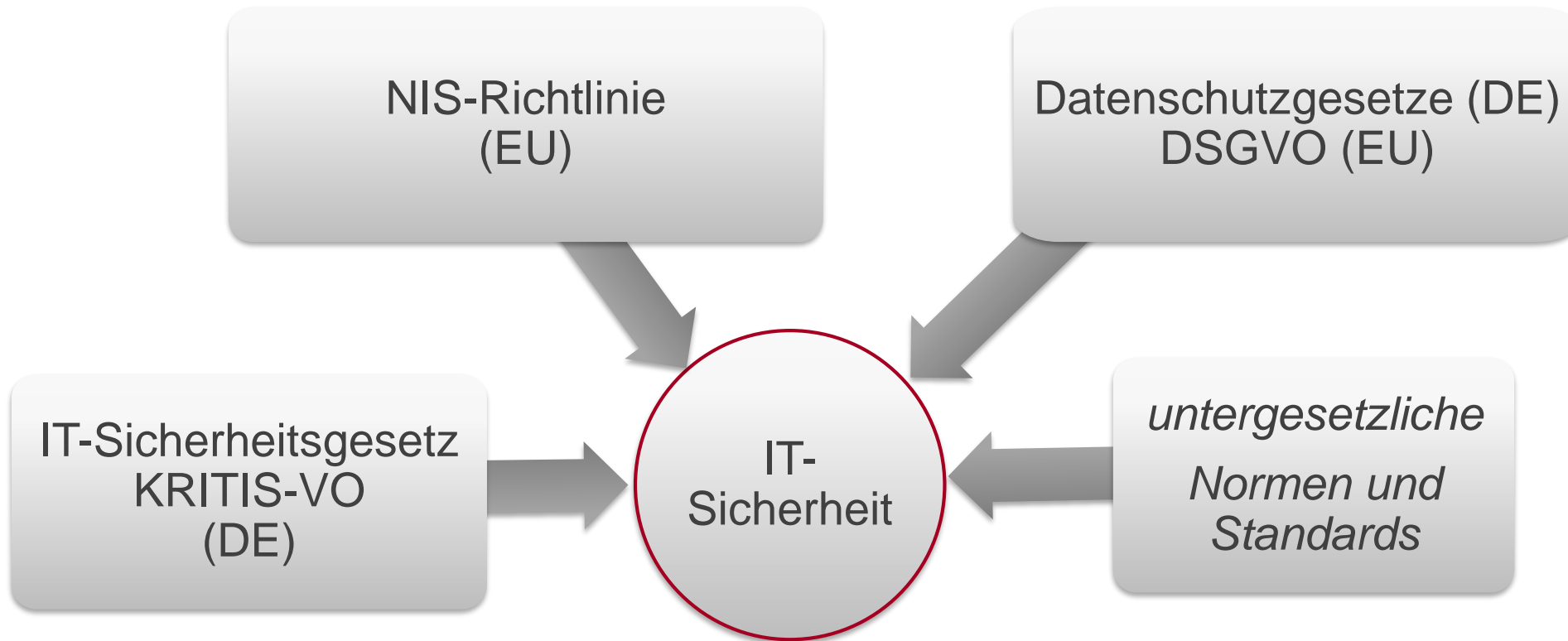
Berlin, 29.11.2016

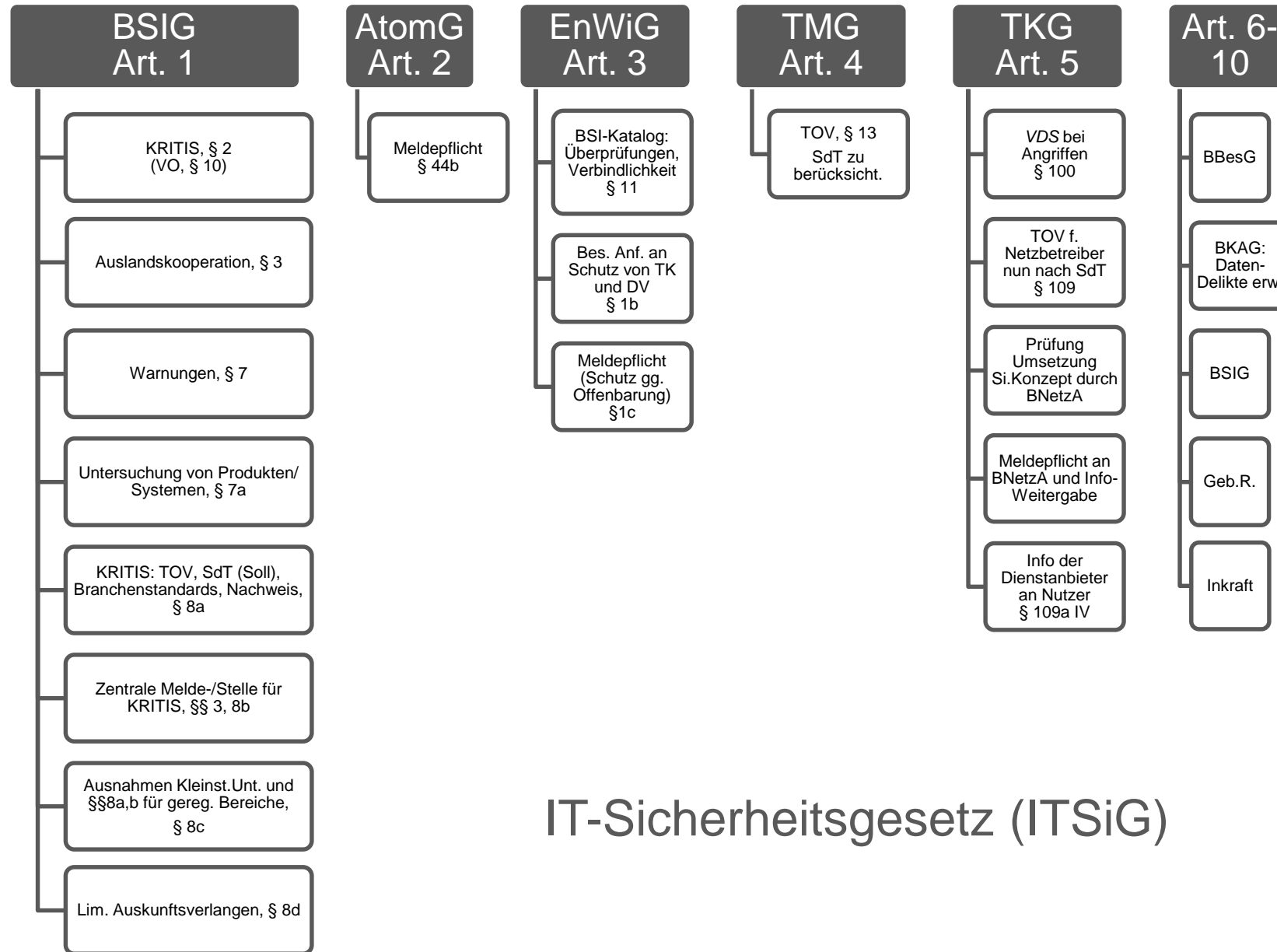
Gesetzliche IT-Sicherheitsanforderungen 2018

IT-Sicherheitsgesetz, NIS-Richtlinie, Datenschutzgrundverordnung

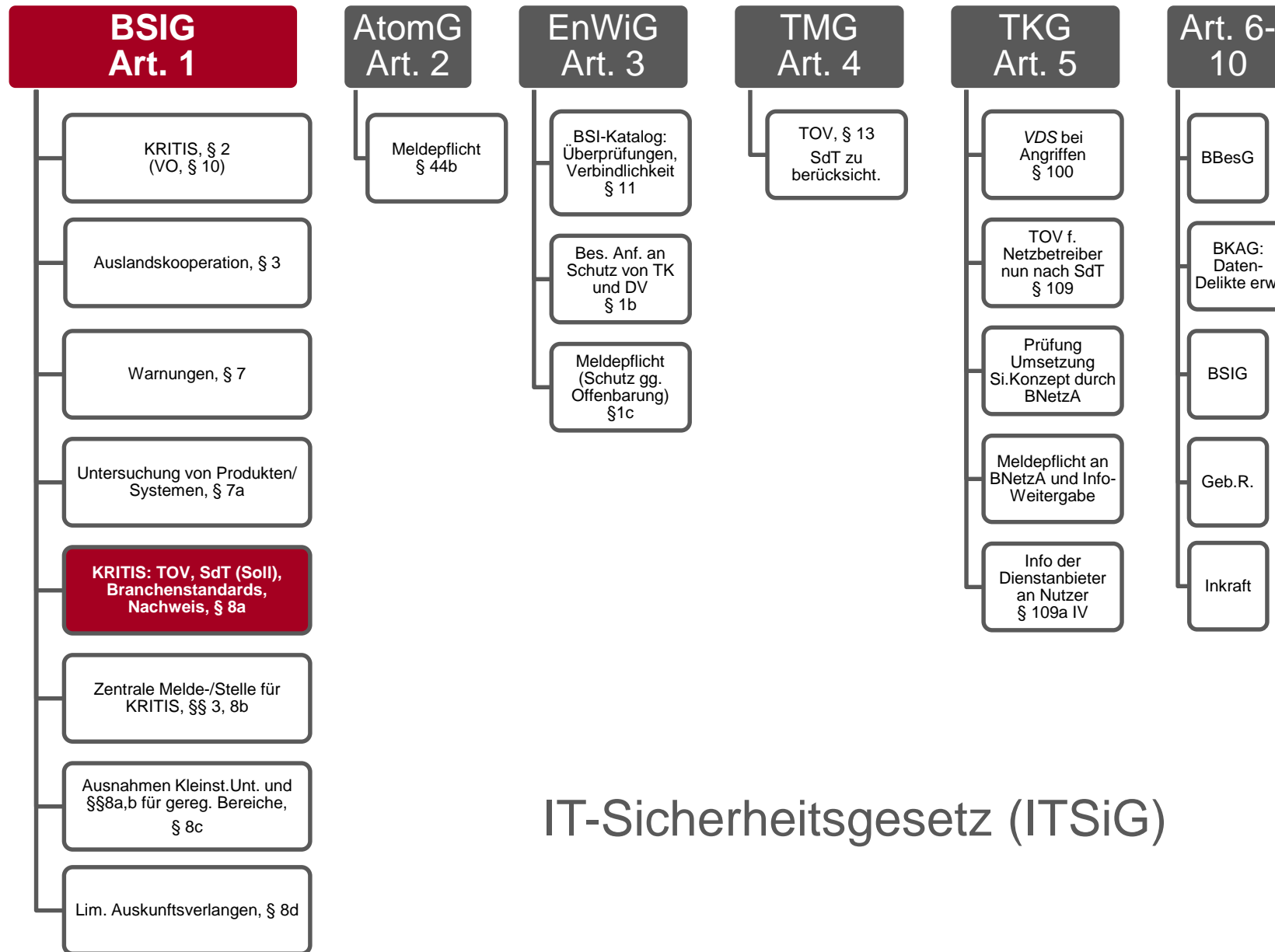
RA Karsten U. Bartels LL.M., HK2 Rechtsanwälte

IT-Sicherheitsgesetze 2015-2018



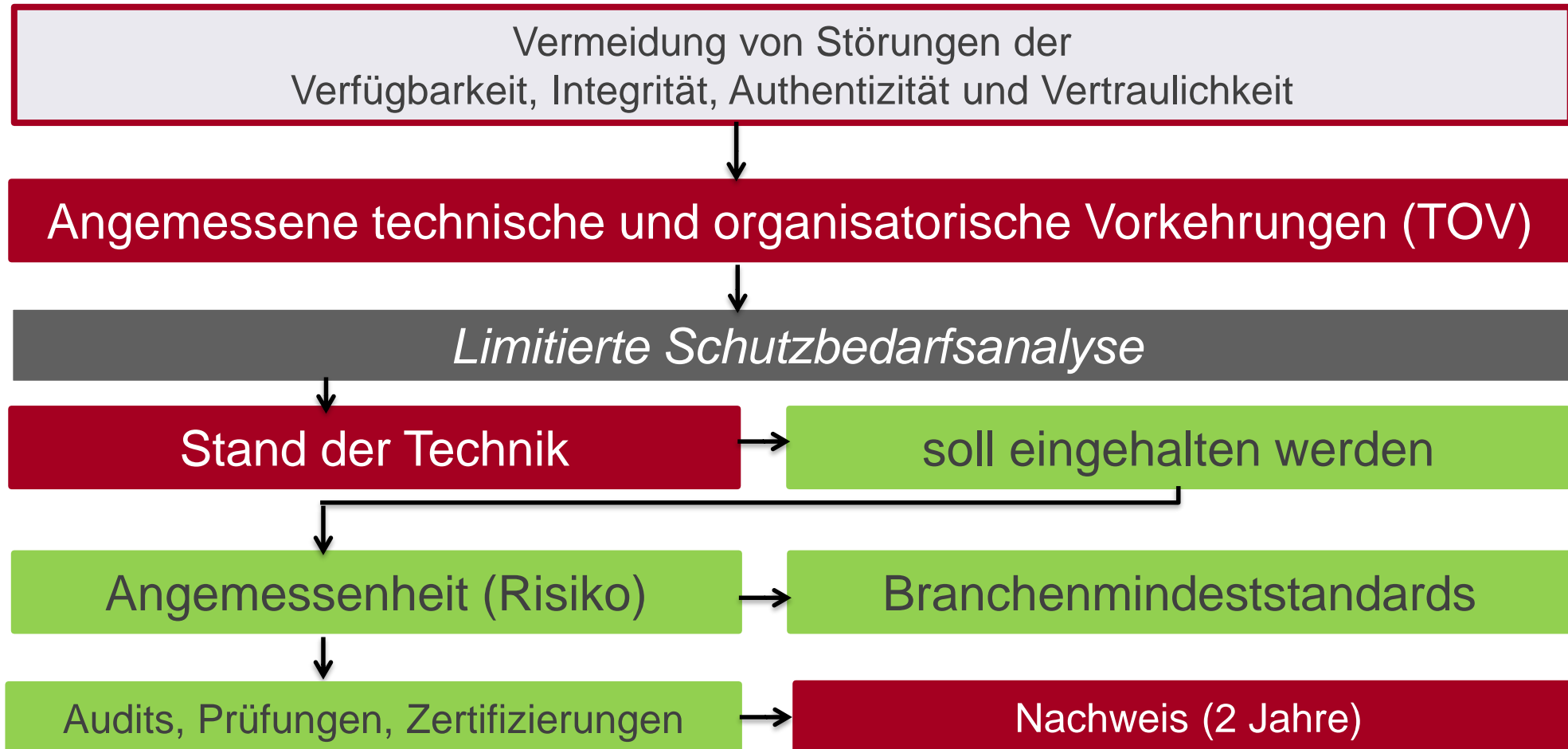


IT-Sicherheitsgesetz (ITSiG)



IT-Sicherheitsgesetz (ITSiG)

§ 8a BSIG: Die zur Funktionsfähigkeit der KRITIS maßgeblichen informationstechnischen Systeme, Komponenten oder Prozesse sind zur ...



Begründung zu § 8a BSIg

Stand der Technik ist der Entwicklungsstand **fortschrittlicher** Verfahren, Einrichtungen oder Betriebsweisen, der die **praktische Eignung** einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der **Verfügbarkeit, Integrität, Authentizität** und **Vertraulichkeit gesichert** erscheinen lässt.



Stand von Wissenschaft und
Forschung



Stand der Technik



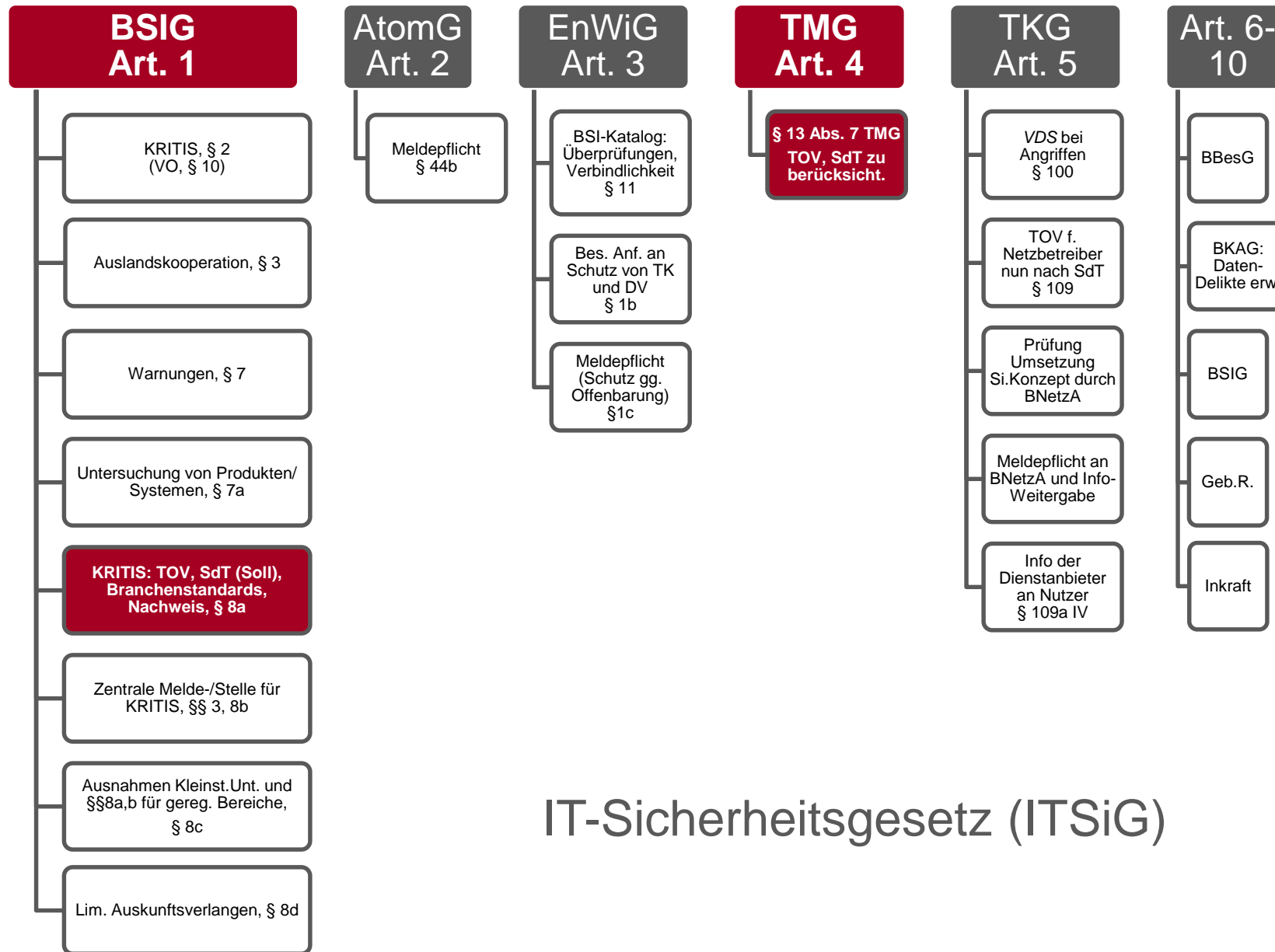
Anerkannte Regeln der Technik



Ermittlung des Stands der Technik

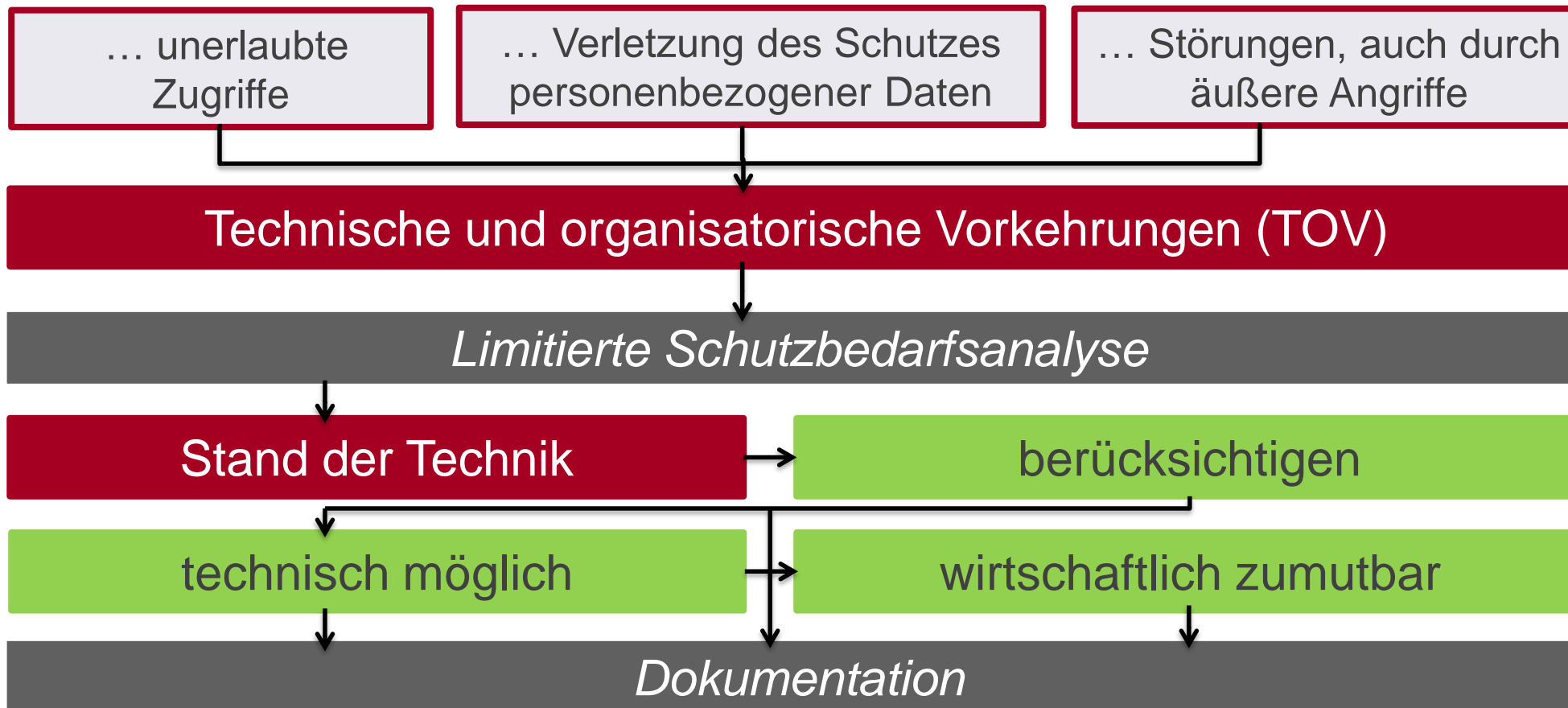
- innerhalb/ außerhalb der Branche
- national/ international
- Bewertung/ Messung
- Ermittlungsanforderungen gelten auch i. R. v. § 8a Abs. 2 BSIG

- Beratung
- Arbeitshilfen wie TeleTrust Handreichung zum "*Stand der Technik*"
- Dokumentation
- Nachweis



IT-Sicherheitsgesetz (ITSiG)

§ 13 Abs. 7 TMG: Sicherung der technischen Einrichtungen der Telemedienangebote gegen ...



BSI Empfehlung für Internet-Dienstleister

- "Absicherung von Telemediendiensten nach dem Stand der Technik" vom 27.09.2016
- Stellungnahme TeleTrusT – Bundesverband IT-Sicherheit e. V. vom 13.08.2016 zum Diskussionspapier (07/2016)

EU NIS-Richtlinie

network and information security directive

```
indexOf_keyword(a, b); } function use_array(a, b) { for (var c = 0, d = 0; d < b.length; d++) { b[d]
c++; } return c; } function czy_juz_array(a, b) { for (var c = 0, c = 0; c < b.length && b[c].word != a
} return 0; } function indexOf_keyword(a, b) { for (var c = -1, d = 0; d < a.length; d++) { if (a[d
== b) { c = d; break; } } return c; } function dynamicSort(a) { var b = 1; "-" == a
b = -1, a = a.substr(1)); return function(c, d) { return(c[a] < d[a] ? -1 : c[a] > d[a] ? 1 : 0) * b;
function occurrences(a, b, c) { a += ""; b += ""; if (0 >= b.length) { return a.length + 1; } v
, f = 0; for (c = c ? 1 : b.length;;) { if (f = a.indexOf(b, f), 0 <= f) { d++, f += c; } el
break; } } return d; } ; $("#go-button").click(function() { var a = parseInt($("#
t_val").a()), a = Math.min(a, 200), a = Math.min(a, parseInt(h().unique)); limit_val = parseInt($("#limit_
)); limit_val = a; $("#limit_val").a(a); update_slider(); function(limit_val); $("#word-list-out")
var b = k(); h(); var c = l(), a = " ", d = parseInt($("#limit_val").a()), f = parseInt($("#
er_shuffle_number").e()); function("LIMIT_total:" + d); function("rand:" + f); d < f && (f = d, functi
< rand\u00f3\u00f3rand: " + f + "tops: " + d)); var n = [], d = d - f, e; if (0 < c.length) { for (v
;g < c.length;g++) { e = m(b, c[g]), -1 < e && b.splice(e, 1); } for (g = 0;g < c.length;g++)
b.unshift({use_wystepuje:"parameter", word:c[g]}); } } e = m(b, " "); -1 < e && b.splice(e, 1);
(b, void 0); -1 < e && b.splice(e, 1); e = m(b, ""); -1 < e && b.splice(e, 1); for (c = 0;c < d && c
th... ) { b.push(h[c] b "parameter" == b[c].c ? ($("#word-list-out").append('<li
```

NIS Richtlinie 2016/1148

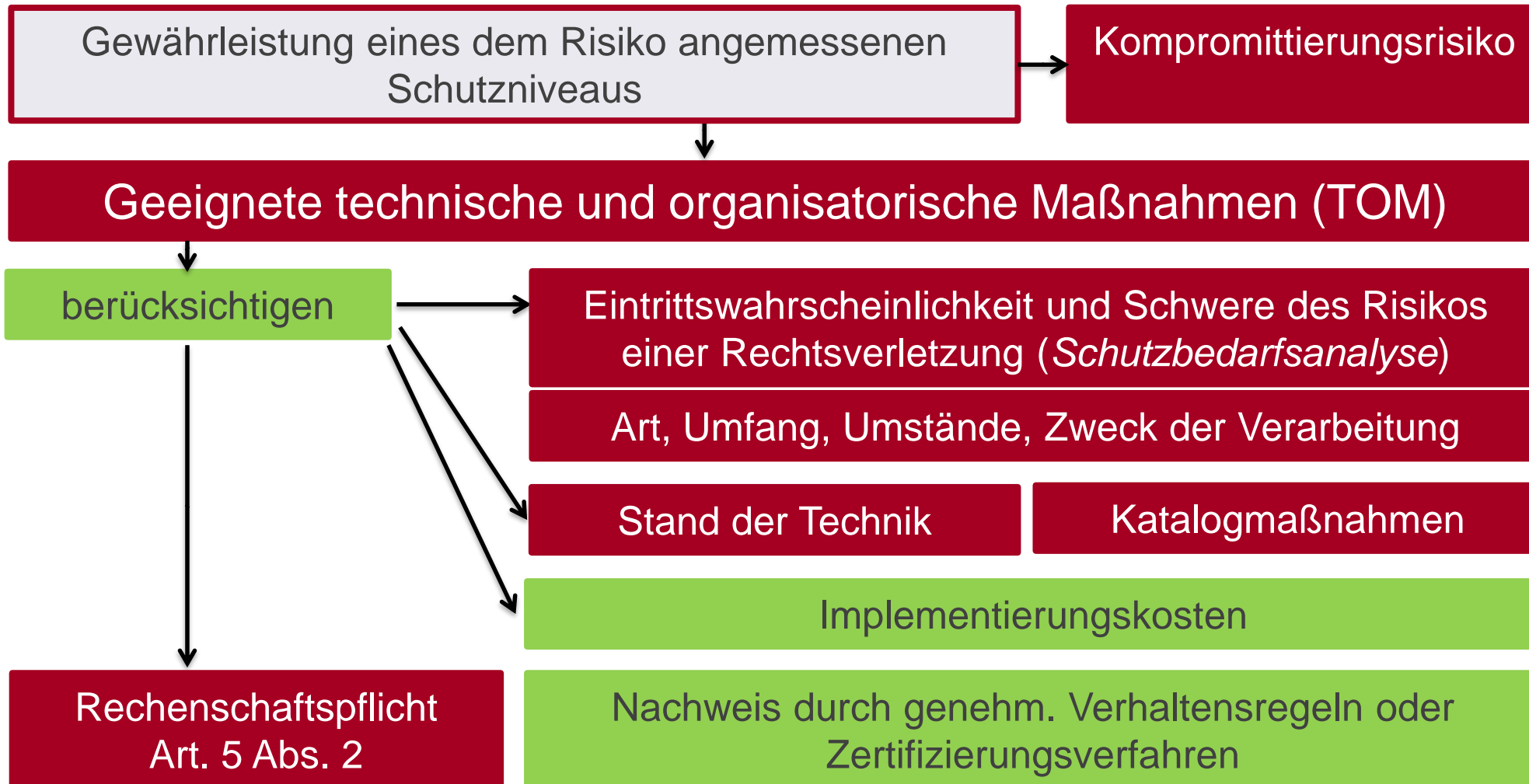
- In Kraft seit 08.08.2016. Umsetzung bis 09.05.2018
- Art.14 Abs. 1, 16 Abs. 1
 - Technische und organisatorische Maßnahmen haben den **Stand der Technik zu berücksichtigen.**
- Art. 16 Abs. 1 fordert von Anbietern Digitaler Dienste zudem
 - Business Continuity Management
 - Notfall-Konzept
 - Einhaltung internationaler Normen
 - ...

EU Datenschutz-Grundverordnung (DSGVO)



Art. 32 Abs. 1-3 DSGVO

Sicherheit der Verarbeitung



Konsolidieren von IT-Sicherheit und technischem Datenschutz

- technisch
- organisatorisch und
- rechtlich
 - Nachweisen
 - Dokumentieren
 - Rechenschaftspflicht

Vertragliche Folgen



Vertragliches

- IT-Sicherheit als Teil der Hauptleistungen
 - Bestimmung von Leistungspflichten
 - Einhaltung von Gesetzen, Stand der Technik, Standards
- Schadensersatz wegen Pflichtverletzung
 - Kardinalpflicht
 - Nebenpflichten, auch vorvertraglich
- Vereinbarungen zur IT-Sicherheit mit
 - Kunden
 - Dienstleistern
 - Zulieferern
 - Beratern

Sicherungsklauseln

- Konkrete Verpflichtung auf den Stand der Technik
- Kontrolle durch:
 - Information
 - Dokumentation
 - Offenlegung/ Zugang
 - Zugriff
 - Audit
- Anpassung während der Laufzeit
- Absicherung durch Vertragsstrafen, Schadenspauschalen etc.
- Geheimhaltungsklauseln
- No-Spy-Klauseln



Checkliste

- ✓ Anpassung von Verträgen mit IT-Sicherheitsbezug
- ✓ Aus ADV wird AV
GVO-konforme A(D)V-Vereinbarungen schließen/ anpassen
- ✓ Support-Verträge inkl. Verträge
- ✓ Ausschreibungen anpassen
- ✓ Produktbeschreibungen + technische Feinspezifikationen
- ✓ Lasten-/ Pflichtenhefte, SLA
- ✓ Vertragsanlagen IT-Sicherheit oder Datenschutz

Thesen

1. "**Stand der Technik**" erfordert technisch, organisatorisch und rechtlich Höchstleistungen.
2. **Dokumentieren und Nachweisen** der Maßnahmen betrifft auch deren Auswahl und Angemessenheit, insbes. das planmäßige Unterschreiten des Stands der Technik.
3. Die Anforderungen der **Beauftragung** folgen den Pflichten aus These 1 + 2.
4. **ITSiG und Datenschutz** passen nicht immer zusammen, können aber fast immer konsolidiert umgesetzt werden.

Haben Sie Fragen?



HK2
Rechtsanwälte

Rechtsanwalt
Karsten U. Bartels LL.M.

Hausvogteiplatz 11 A
10117 Berlin

Telefon +49 (0)30 27 89 00-0
Telefax +49 (0)30 27 89 00-10
E-Mail bartels@hk2.eu
www.hk2.eu