Informationstag "Umsetzung des IT-Sicherheitsgesetzes in der Unternehmenspraxis"

Gemeinsame Veranstaltung von TeleTrusT, bevh und BISG

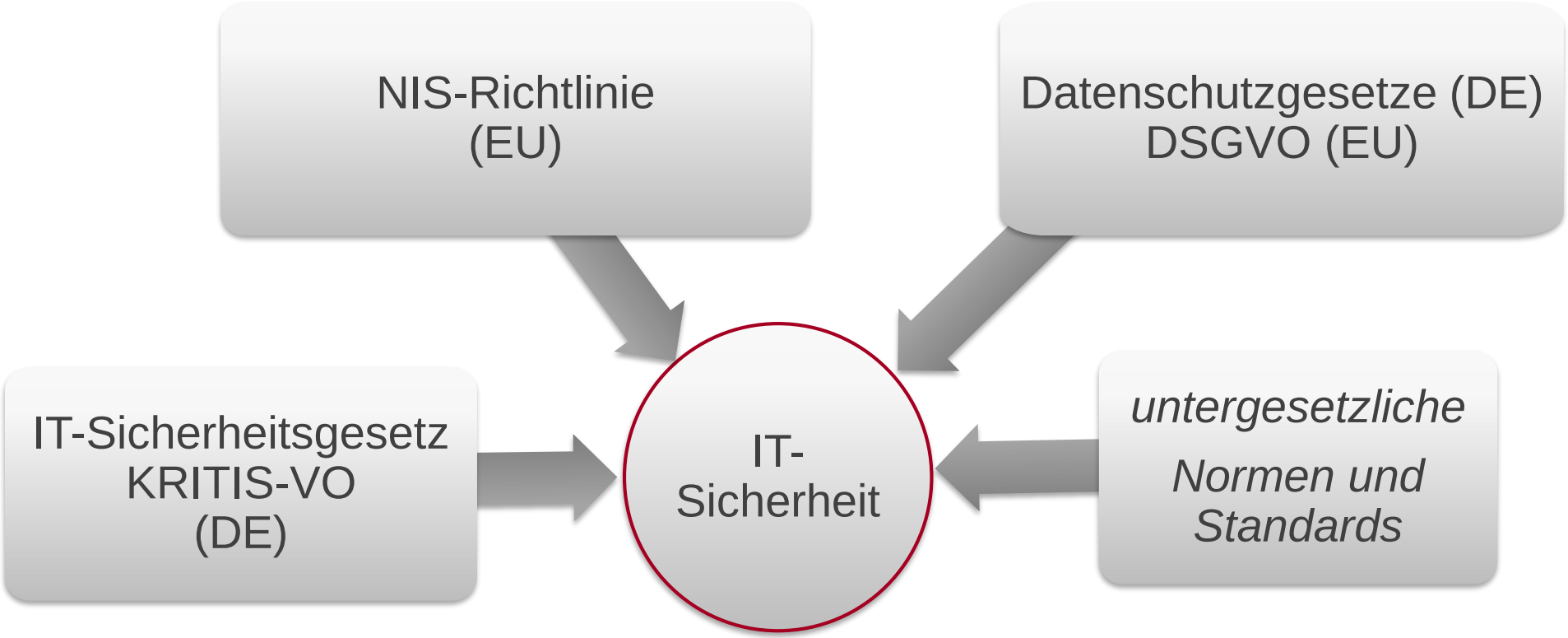
Berlin, 29.11.2016

Gesetzliche IT-Sicherheitsanforderungen 2018

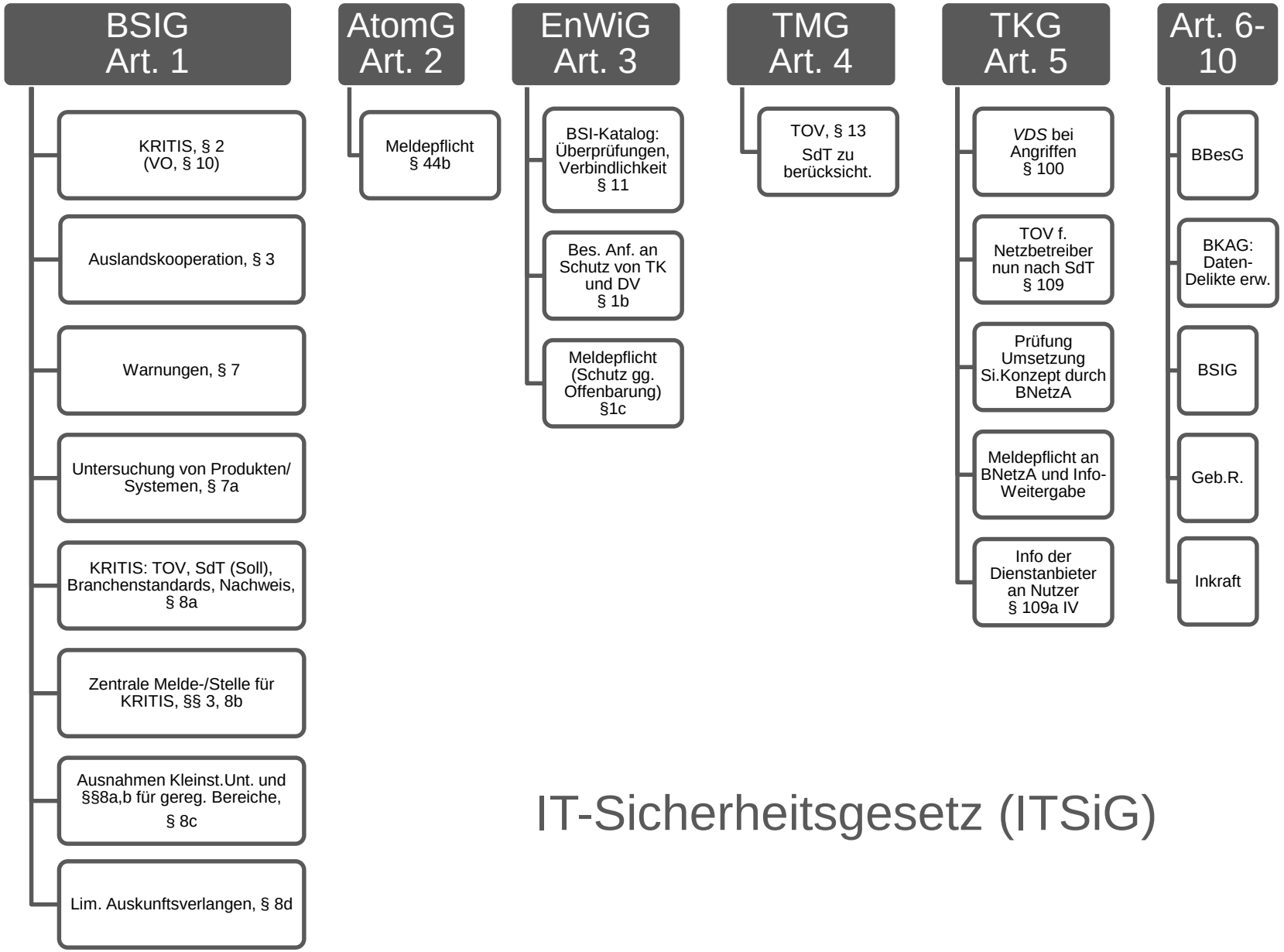
IT-Sicherheitsgesetz, NIS-Richtlinie, Datenschutzgrundverordnung

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

IT-Sicherheitsgesetze 2015-2018

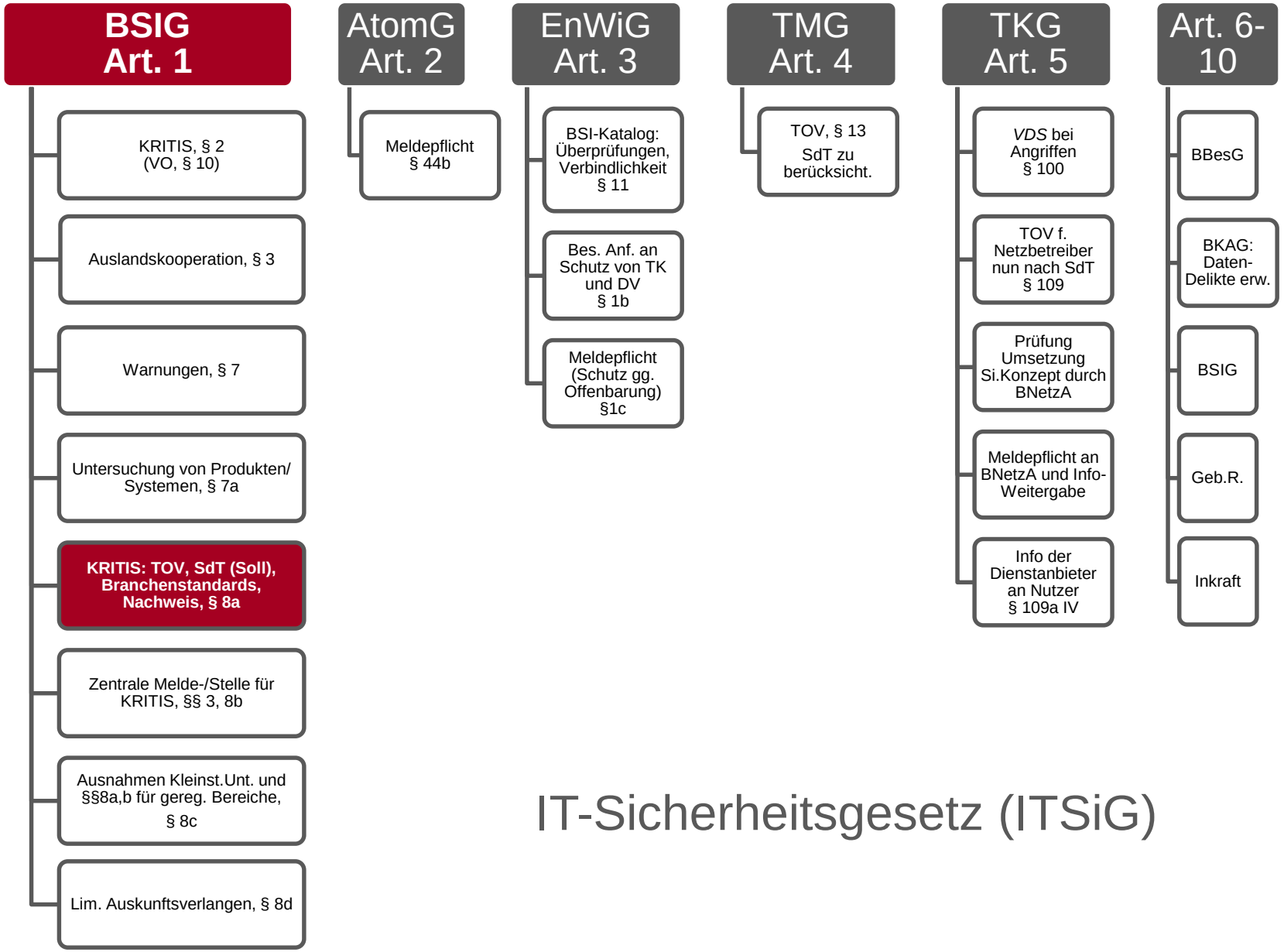


HK2 Rechtsanwälte



IT-Sicherheitsgesetz (ITSiG)

HK2 Rechtsanwälte



IT-Sicherheitsgesetz (ITSiG)

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

HK2 Rechtsanwälte

HK2 Rechtsanwälte

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.

HK2 Rechtsanwälte

Stand von Wissenschaft und Forschung

Stand der Technik

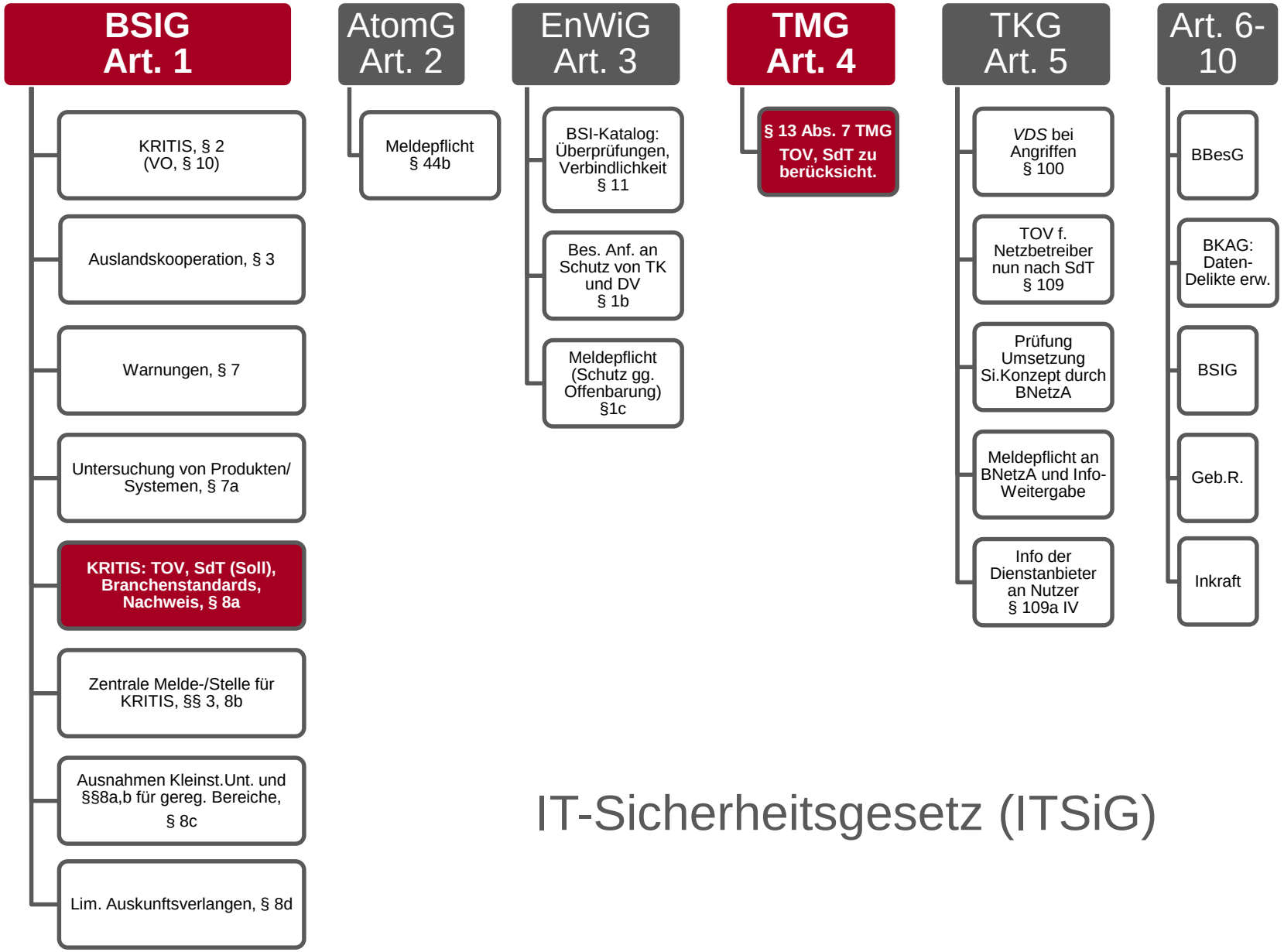
Anerkannte Regeln der Technik

Ermittlung des Stands der Technik

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

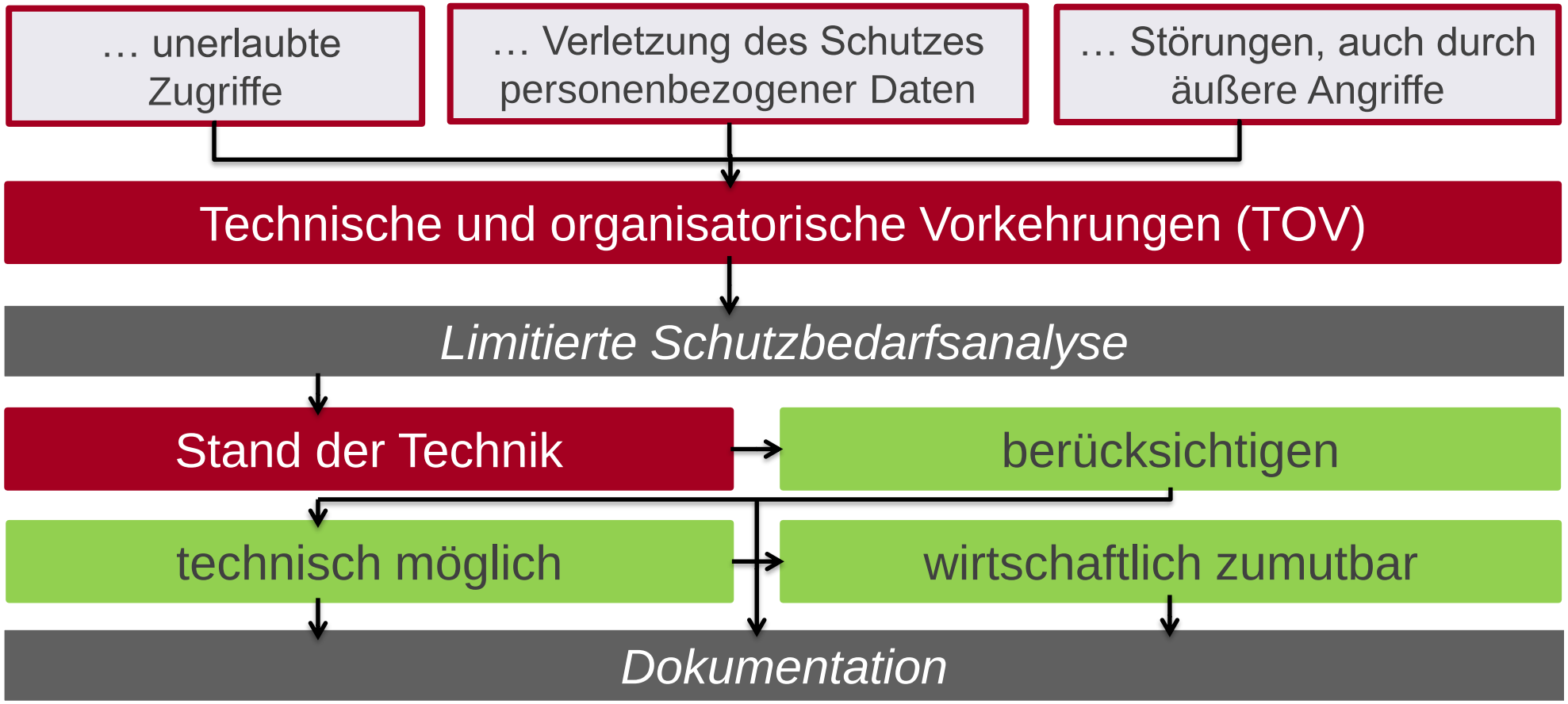
- Beratung
- Arbeitshilfen wie TeleTrusT Handreichung zum "*Stand der Technik*"
- Dokumentation
- Nachweis

HK2 Rechtsanwälte



IT-Sicherheitsgesetz (ITSiG)

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



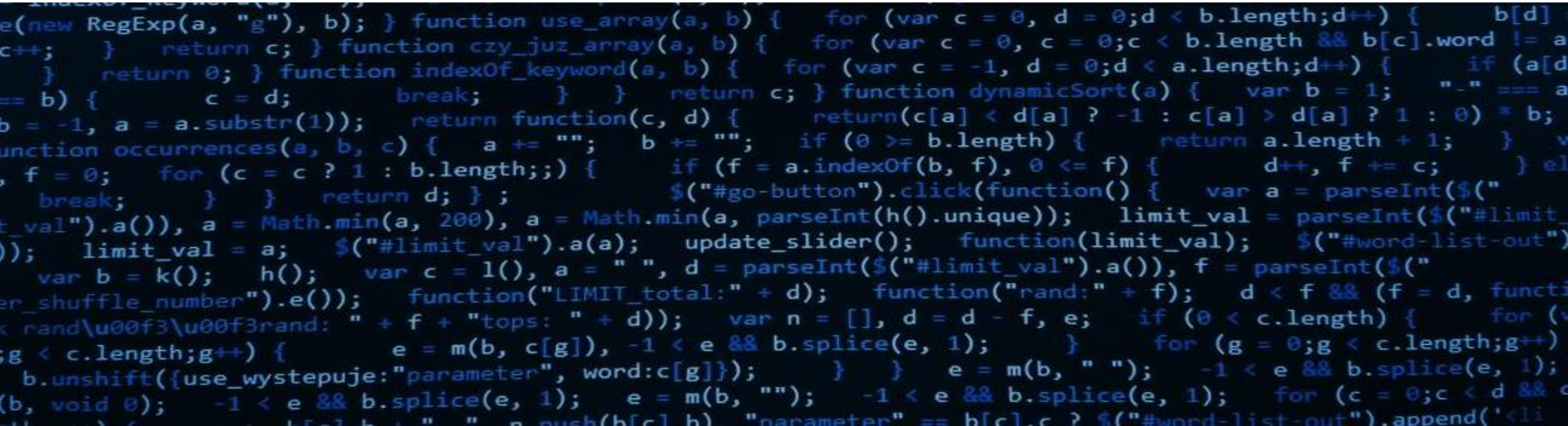
HK2 Rechtsanwälte

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)

HK2
Rechtsanwälte

EU NIS-Richtlinie
network and information security directive



HK2 Rechtsanwälte

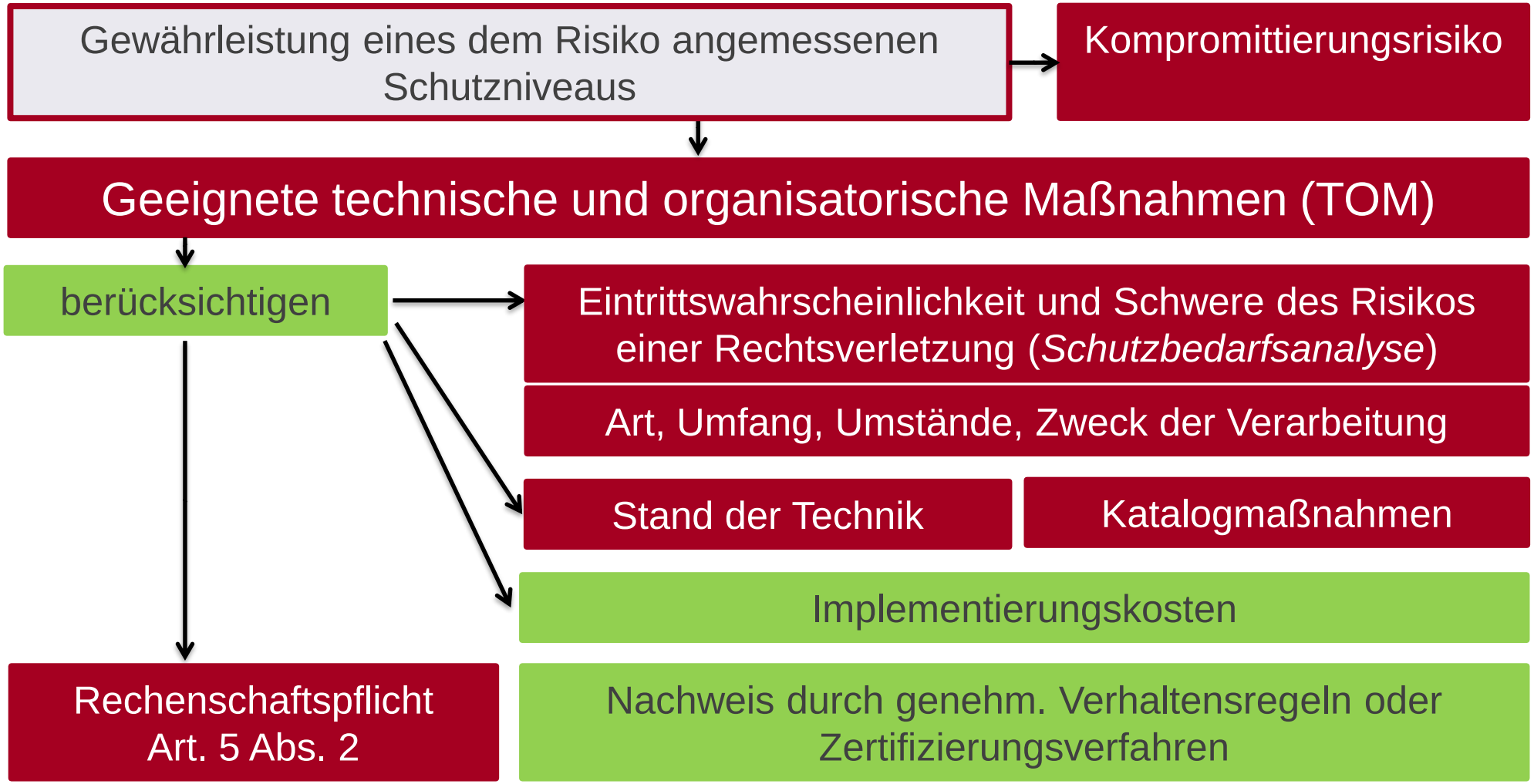
NIS Richtlinie 2016/1148

- 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
  - ...

HK2
Rechtsanwälte

EU Datenschutz-Grundverordnung (DSGVO)

Art. 32 Abs. 1-3 DSGVO
Sicherheit der Verarbeitung



Konsolidieren von IT-Sicherheit und technischem Datenschutz

HK2 Rechtsanwälte

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

HK2
Rechtsanwälte

Vertragliche Folgen

HK2
Rechtsanwälte

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

HK2 Rechtsanwälte

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

HK2
Rechtsanwälte

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

HK2 Rechtsanwälte

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?