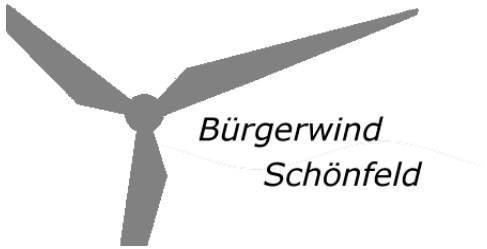
Informationssicherheit in Energienetzen

Georg Sven Lampe



&

Ingenieurbüro Massner

17. Mai 2018

Übersicht

Terminologie

- **Informationssicherheit**
  - Gewährleistung von Schutzzielen
- **Schutzziel**
  - ein mindestens zu erreichendes Sicherheitsniveau
  - Klassifizierung: **Privatsphäre**, **Sicherheit**, **Schutz**
- **Privatsphäre**
  - nicht-öffentlicher Bereich zur Wahrnehmung des Rechtes auf freie Entfaltung der Persönlichkeit unbehelligt von äußeren Einflüssen [Art. 8 EMRK] [Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG]
- **Sicherheit**
  - ein von unvertretbaren Risiken freier Zustand
- **Schutz**
  - etwas, was eine Gefährdung abhält oder einen Schaden abwehrt

Terminologie

- **Bedrohung**
  - ernste Gefährdung mit der bloßen Möglichkeit des Schadenseintritts
- **Risiko**
  - Ereignis mit möglicher negativer/positiver Auswirkung
- **Gefährdung**
  - (tech.) Möglichkeit des räumlichen/zeitlichen Zusammentreffens eines Schutzgutes mit einer Gefahrenquelle (potentielle Schadensquelle) [ISO/IEC Guide 51]
- **Schaden**
  - materieller/immaterieller Nachteil durch ein Ereignis

Energiewende und Marktintegration

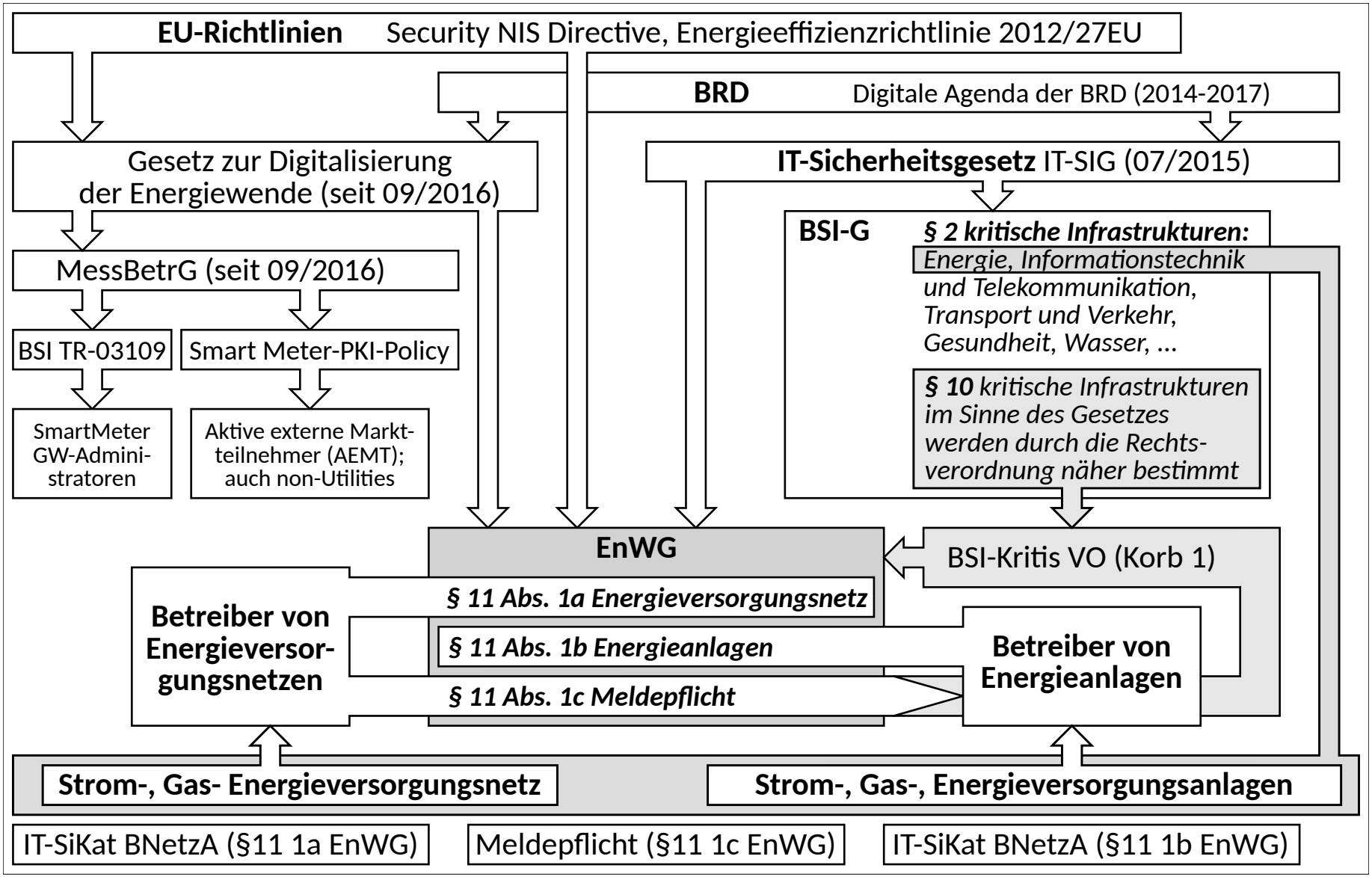
- **Erneuerbare Energien Gesetz (EEG)**
  - Regelung der bevorzugten Einspeisung von Strom aus "erneuerbaren Energien" (EE)
  - Festlegung von Rahmenbedingungen der Stromversorgung
  - Steuerung des Energienetzes
- **Energiewirtschaftsgesetz (EnWG)**
  - Definition und Anforderungen an Sicherheitsarchitektur der Funktions- und Energieverteilungseinrichtungen von intelligenten Netzen (Smart Grid) sowie Erzeugungs- und Verbrauchseinrichtungen durch zu erfüllende Sicherheitskataloge (IT-SiKat BNetzA)
- **Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)**
  - ISO 27001 Umsetzung aus Verpflichtung[1] nach BGBl Teil 1 Nr. 31

[1] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), Bundesgesetzblatt Teil 1 Nr. 31 S. 1324-1331 (17.7.2015, ausgegeben am 24.7.2015)

Energiewende und Marktintegration

- **BSI-Gesetz (BSIG)**
  - Definitionen und Anforderungen der Informationssicherheit auf nationaler Ebene durch Einordnung kritischer Infrastrukturen (KRITIS) nach §§ 2 und 10 BSIG
- **IT-Sicherheitskataloge (IT-SiKat)**
  - nähere Anforderungen an Funktionen/Ausstattung der Sicherheitsarchitektur von KRITIS-Betreiber durch Einführung eines ISMS gemäß DIN ISO/IEC 27001 und Zertifizierung (§11 1a EnWG bis 31.01.2018, §11 1b EnWG innerhalb 1,5 Jahren nach in Kraft treten der Rechtsverordnung gemäß § 10 Absatz 1 BSIG) mit Meldepflicht gemäß §11 1c EnWG
- **Marktintegration**
  - Ertüchtigung des vorhandenen EDM-Systems und Dienstleistungsverkauf an Dritte als weiterer Geschäftszweig

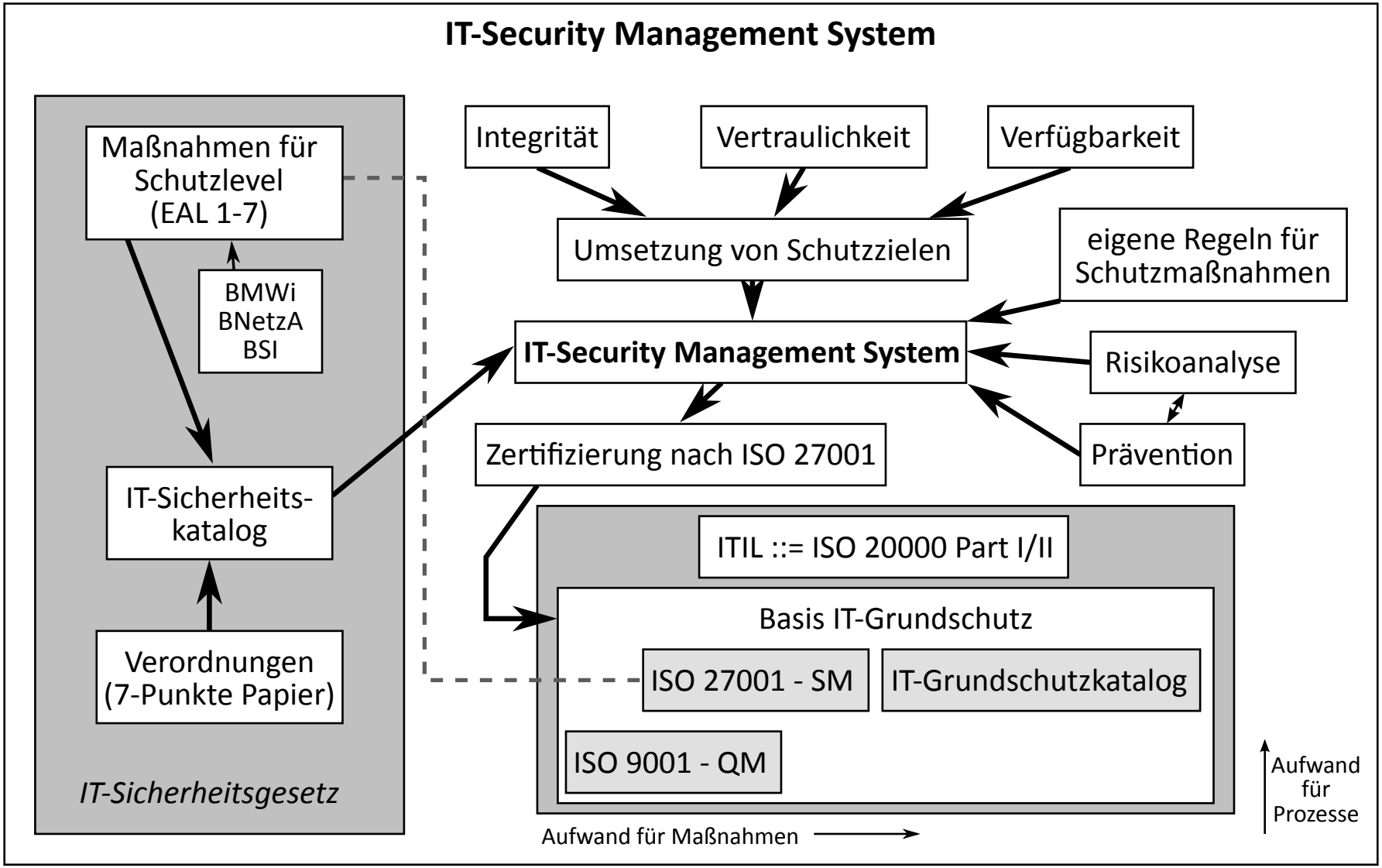
Übersicht gesetzlicher Pflichten - EnWG, BSIG, SiKat, ISMS



Status QUO - Schwachstellen, Bedrohung, Gefährdung, Risiken

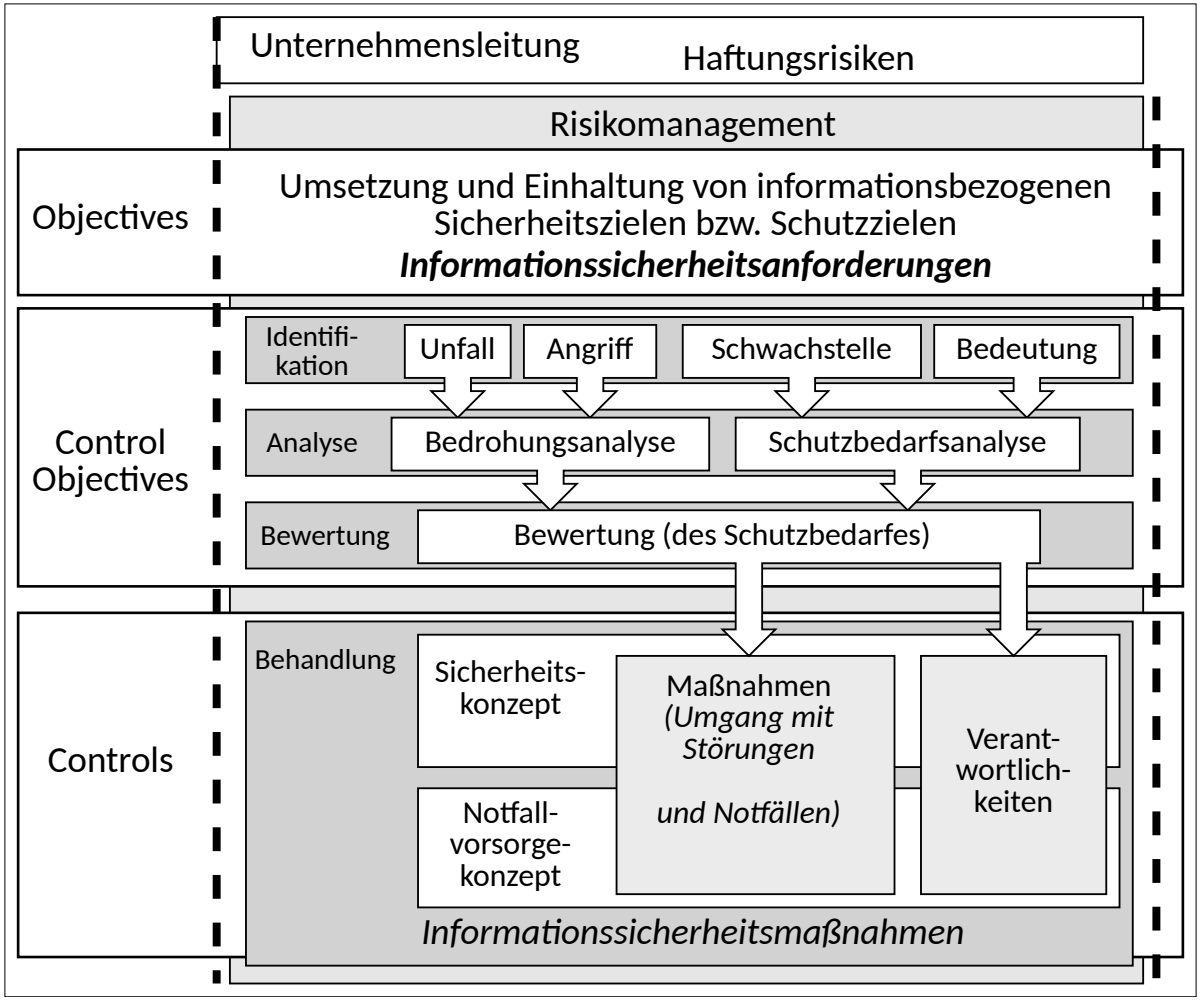
- Status QUO
  - Ausnutzung von Protokollschwachstellen (nicht verschlüsselt, keine Integritätsprüfung)
  - Aktives Verbergen entdeckter Schwachstellen in Hard- und Software (Staatstrojaner)
  - nicht bestimmungsgemäße Nutzung von IKT-Systeme wegen fehlender operationalisierte Prozesse (physisch, umgebungsbezogen)
  - Angriffsszenarien mit steigender Komplexität zur Datenmanipulation und -überschreibung
  - etc.

Regelwerk



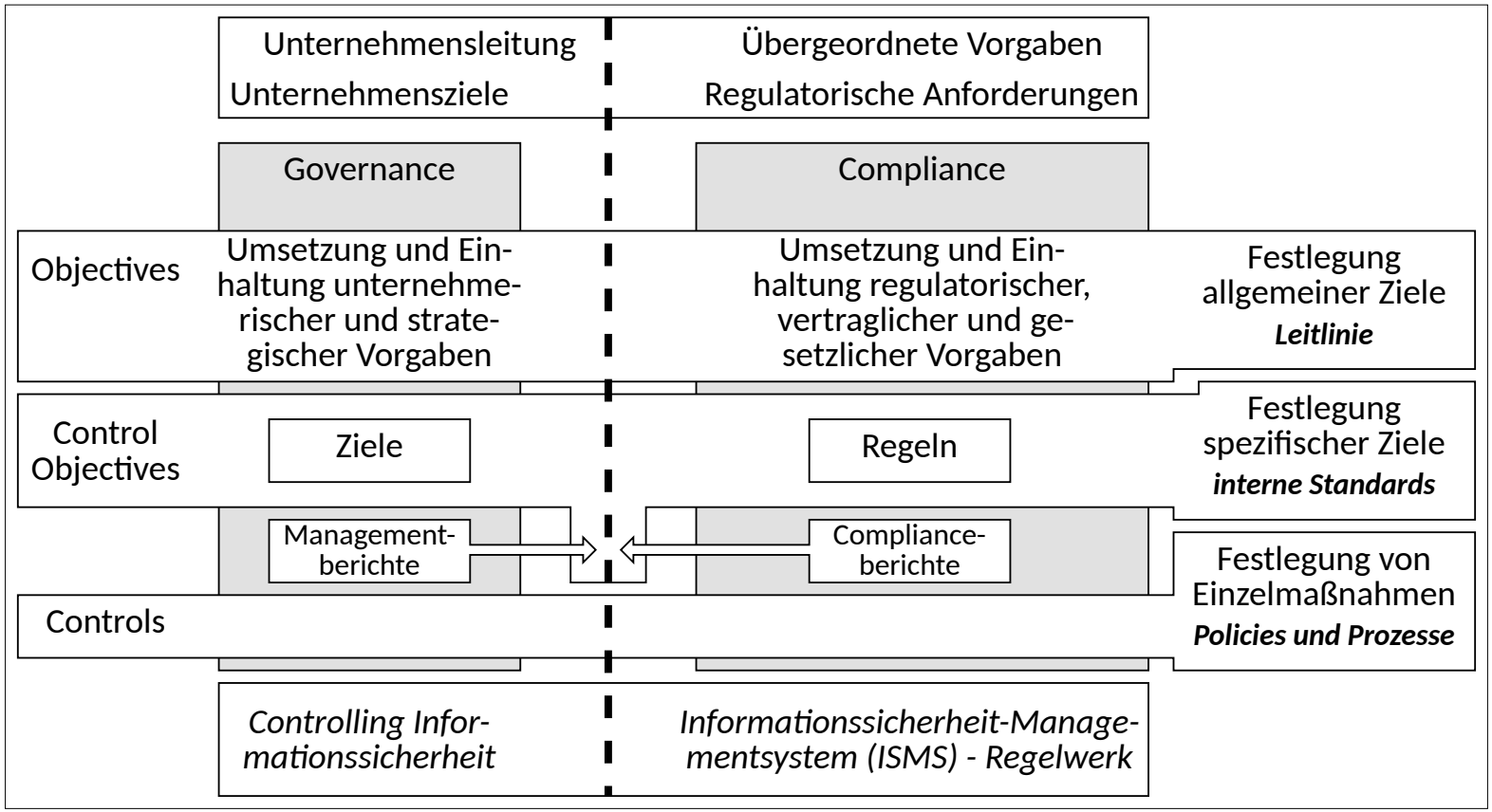
Einordnung des informationstechnischen Sicherheitsmanagementsystems - ISMS

Regelwerk



ISMS-Regelwerk: Governance, Compliance, Riskmanagement

Regelwerk

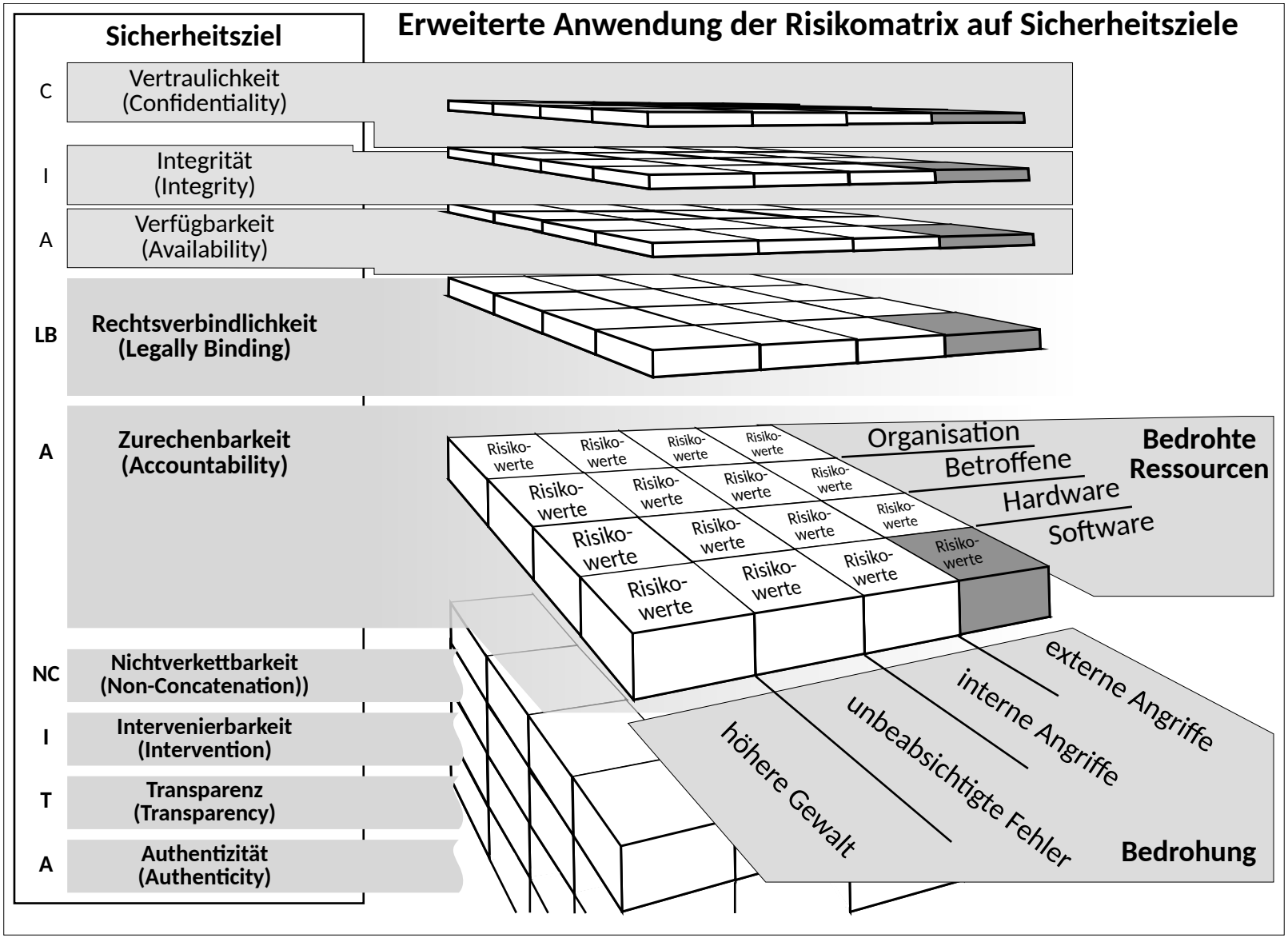


ISMS-Regelwerk: Governance, Compliance, Riskmanagement

Methoden der Risikoanalyse

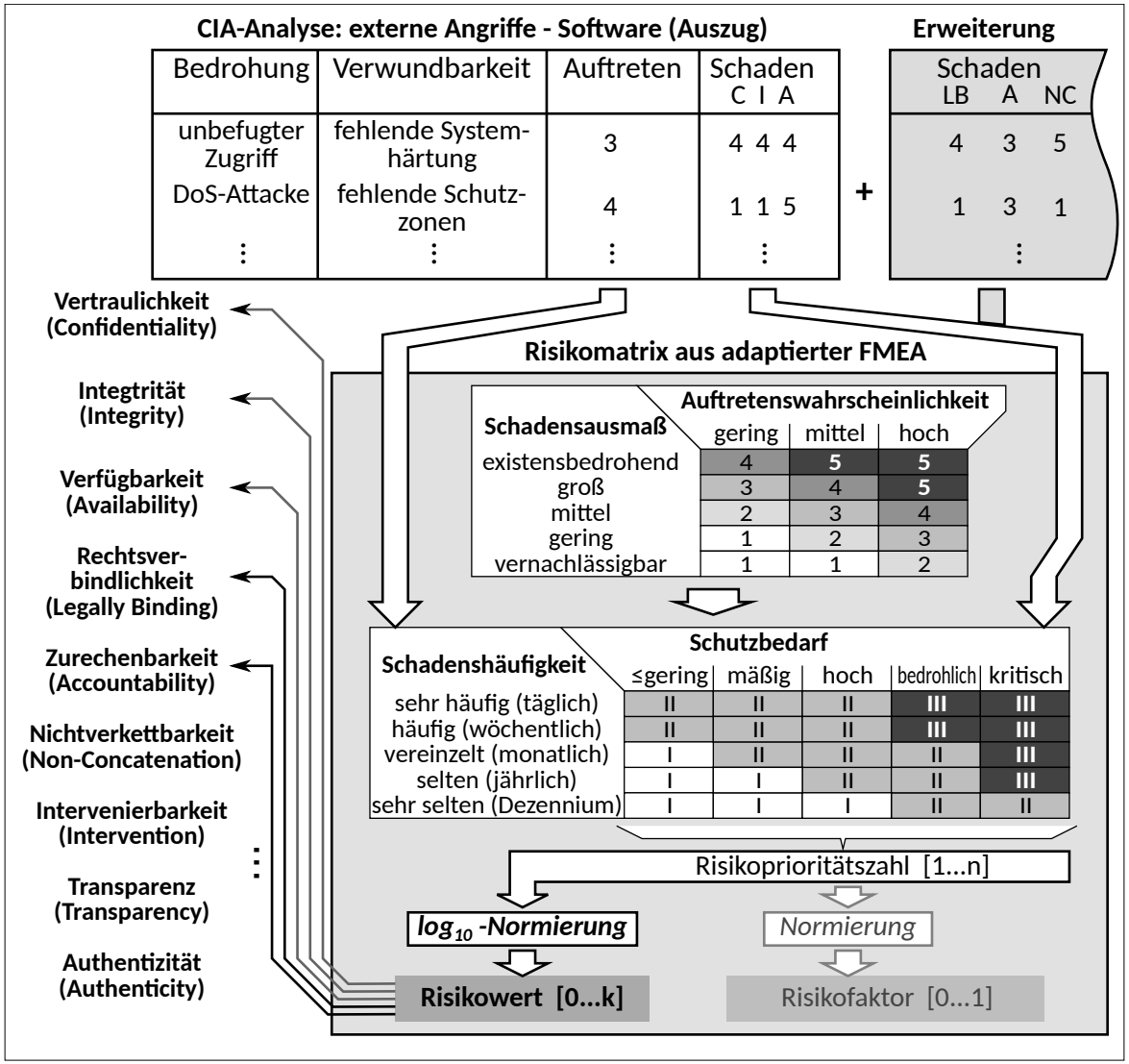
- Risikoanalyse aus adaptierter FMEA mit Schutzzielerweiterung
  - Schutzzielerweiterung (Authentizität, Intervenierbarkeit, Nichtverkettbarkeit, Transparenz) und bei organisatorischen Prozessen und technischen Maßnahmen (z. B. Erwartungswert aus Messwertmodellierung, Risikoreduktion durch autorisierte Anlagenregelung)
  - Aufschlüsselung möglicher Abhängigkeiten zwischen betroffener Ressource und Bedrohung je Schutzziel
  - Darstellung der Risikowerte wichtungsfrei in logarithmischer Form (Basis 10)
  - Standardisierung der Funktions- und Fehlfunktionsnetze
  - Standardisierung organisatorischer Prozesse und technischer Maßnahmen

Anwendung der Risikomatrix



Erweiterte Anwendung der Risikomatrix auf Schutzziele der Informationssicherheit

Anwendung der Risikomatrix



Klassifizierung nach Sicherheitszielen

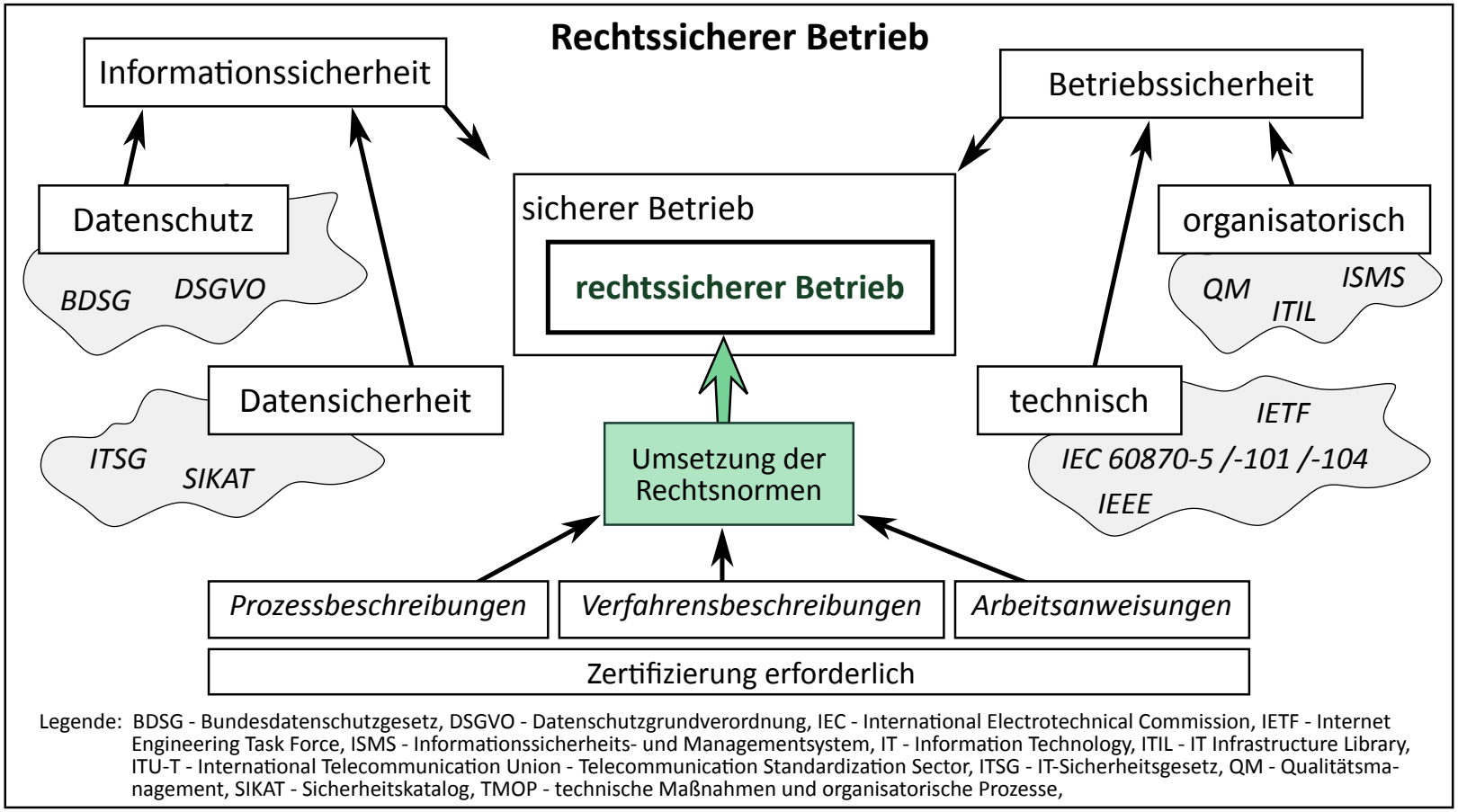
Betrieb des ISMS

- Aufteilung und Klassifizierung der Schutzmaßnahmen
  - Technische Maßnahmen (TM): betreffen die physische und logische Sicherheit der Hard- und Software
  - Personelle Maßnahmen (PM): dienen der Sicherheit ggü. eigenem und fremden Personal
  - Organisatorische Prozesse (OP): optimieren und verbessern Prozesse und Arbeitsabläufe
  - Sicherheitsmaßnahmen klassifiziert nach präventiv, aufdeckend, korrigierend
- Operationalisierung der Schutzmaßnahmen
  - Gliederung des Schutzbedarfs unter Berücksichtigung von Vererbung (Maximum-Prinzip, Kumulations- und Verteilungseffekt)
  - Sicherheitsmaßnahmen standardisiert und zentralisiert (z. Bsp. JIRA Service Desk als Teil des Security Block Gateways)
  - Sicherheitsmaßnahmen nach dem Defense-in-Depth-Prinzip mehrstufig zu etablieren

Haftung

	Endverbraucher	EVU-Störer	Dienstleister
Schadensfall	Versorgungsunterbrechung/-störung	Versorgungsunterbrechung durch Cyberangriff	Versorgungsstörungrung wg. mangelhafter Wartung, fehlerhafter SW
Haftungsgrundlage	§18 NAV/NDAV: Vermögensschädenhaftung bei Vorsatz/grober Fahrlässigkeit, begrenzte Haftung für Sachschäden (ggfs. HaftPflG/ProdHaftG)	§823 BGB: Deliktrecht, Haftung gegenüber Endverbraucher idR. zugleich strafrechtliche Haftung des Störers	Dienstleistungsvertrag
Haftung nach DSGVO/BDSG ab 05/2018 für jedes Unternehmen			
Zivilrechtlich nach Art. 82 DSGVO und §83 BDSG 2018	Verschuldensvermutung: ersatzpflichtig für immaterielle Schäden	Straf- und Bußgeldvorschriften nach Art. 83 DSGVO §§ 41 ff. BDSG 2018	Unbefugte Zugänglichmachung - personenbezogener Daten ist strafbar
Art. 83 DSGVO: Bußgeldverstöße bis zu 20 Mio. EUR oder 4 Prozent des Jahresumsatzes			

Zusammenfassung



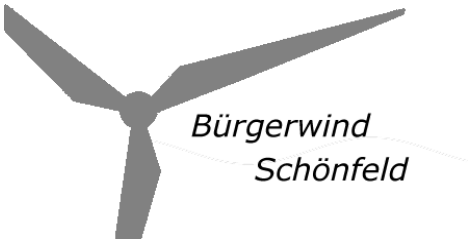
Anhängigkeiten und Voraussetzungen zur Herstellung eines rechtssicheren Betriebes

Ausblick

- **branchenspezifisch standardisierte, klassifizierte und regulatorische Sicherheitsmaßnahmen für ein einheitliches und angemesssenes Sicherheitsniveau der IKT-Infrastruktur und Arbeitsabläufe**
- **gesamtheitliche Klassifizierung und Realisierungstiefe aller Prozess- und Leistungsbestandteile**
- **branchenspezifisch konforme Sicherheitsorganisation der Betreibergruppen sowie Auditverfahren unter Anwendung der erweiterten Risiko-Matrix**
- **systemorientierte Verteilnetz-Automatisierung der Ein- und Ausspeisung für alle Marktakteure zur Erhaltung der Netzstabilität sowie Gewährleistung des effizienten Netzbetriebes**

Danke für Ihre Aufmerksamkeit

Haben Sie Fragen?



schoenfeld@buergerwind-uckermark.de
+49 (0) 3331 298 9594

INGENIEURBÜRO MASSNER

E-mail: massner@hftl.de
+49 (0) 35325 1685-27