



# ISMS in der Energiebranche

Matthias Hofherr, 20.05.2015

# Gefahrenlage



## Blackout?

*“I’m here to tell you that your cyber systems continue to function and serve you not due to the expertise of your security staff but solely due to the sufferance of your opponents”*

Brian Snow, 2012

# Gesetzeslage



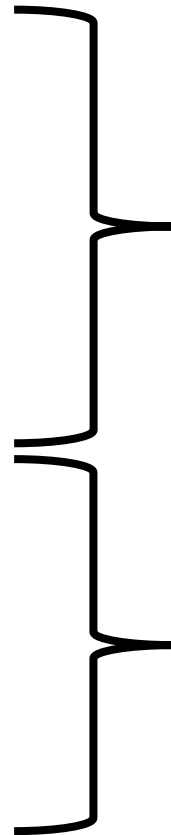
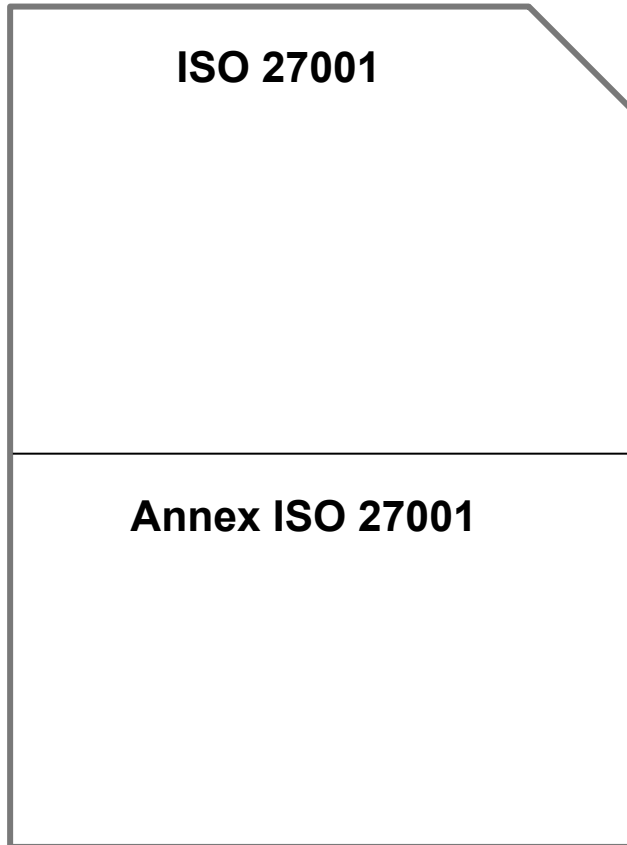
## IT-Sicherheitskatalog

- Für Netzbetreiber (Netzsteuerelemente)
- ISMS nach DIN ISO/IEC 27001
- DIN SPEC 27009 (heute: ISO/IEC TR 27019)
- Zertifizierung

## IT-Sicherheitsgesetz

- Für Betreiber kritischer Infrastrukturen
- Angemessene organisatorische und technische Vorkehrungen (Mindestanforderungen) -> ISMS
- Nachweis alle 2 Jahre (Audits, Prüfungen, Zertifizierungen)

# ISMS

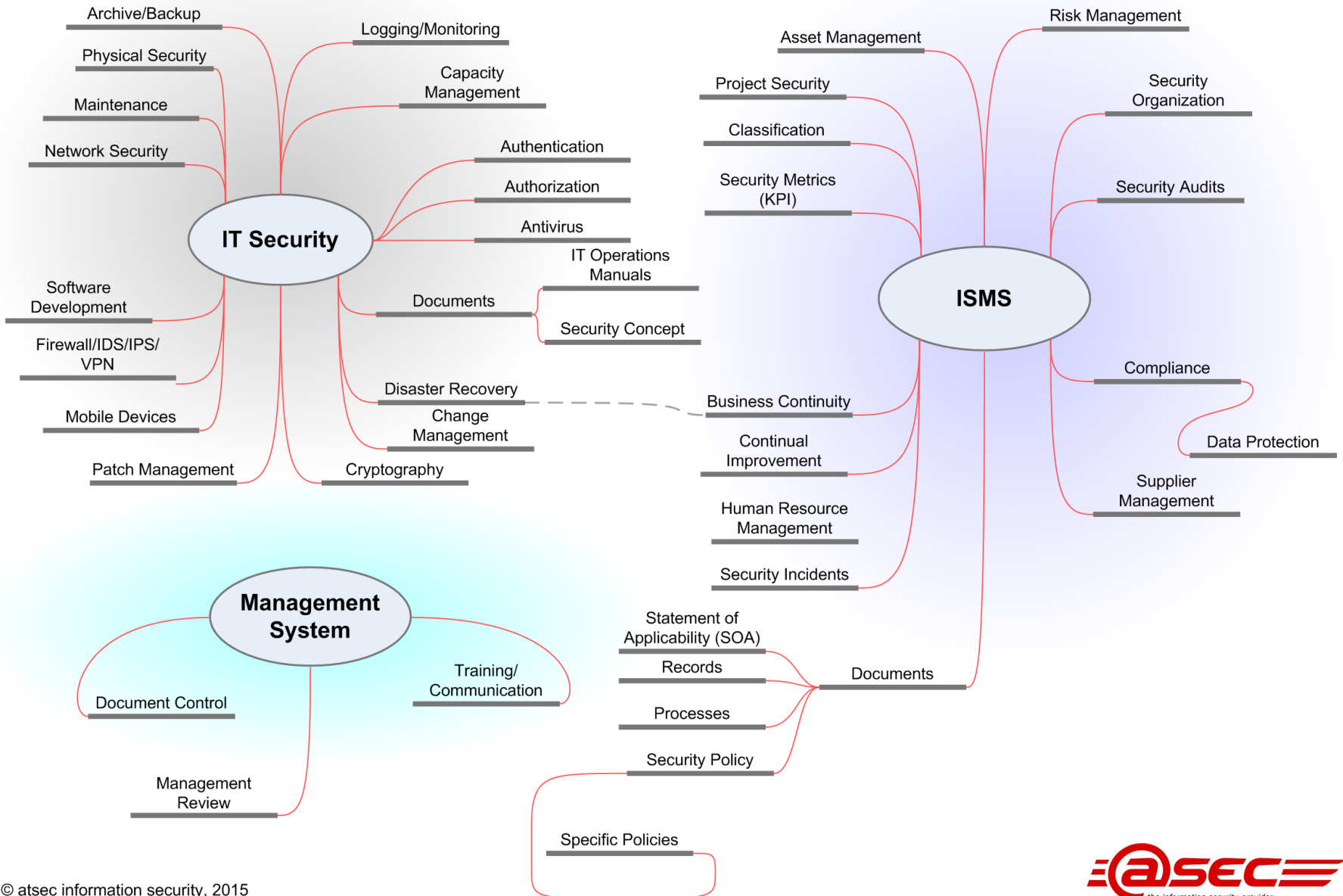


**Anforderungen an ein ISMS**

**Annex: Maßnahmenkatalog  
„Best Practice“ in ISO 27002**

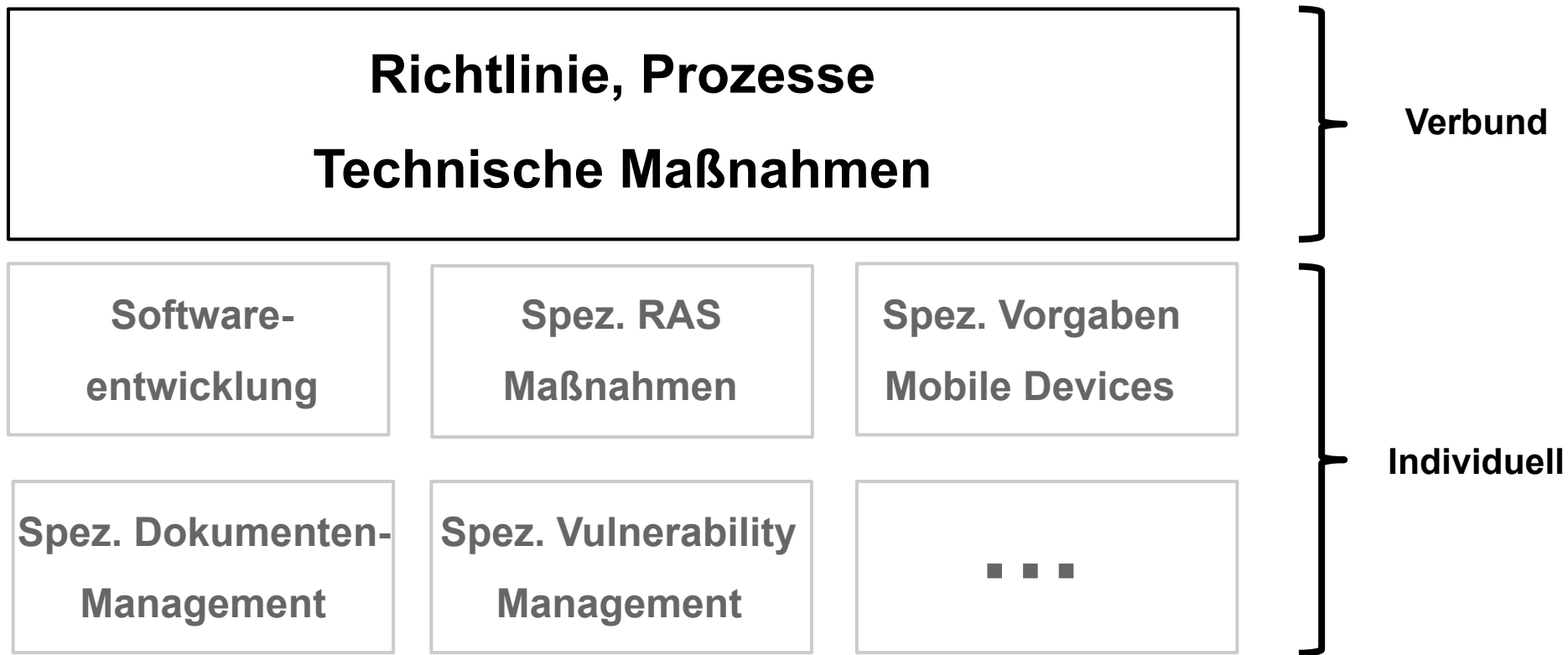
**Energiebranche: Ergänzung ISO/IEC TR 27019**

# ISMS



# Verbund-ISMS

## Implementierung



# Verbund-ISMS

## Zertifizierung

- Steuernde Institution
- Durchgreifende Wirkung bzgl. ISMS (Audits ...)
- Verbindliche Regelungen
- Audit: Steuernde Institution + Stichprobenanteil

## Fazit:

- Machbar für einen begrenzten Teilnehmerkreis
- Abstimmung mit Zertifizierungsstelle notwendig



# Kontakt



**Matthias Hofherr**

**Chief Operating Officer**

atsec information security GmbH  
Steinstraße 70  
81667 München, Germany  
[www.atsec.com](http://www.atsec.com)

Tel: +49 89 442 49 830  
Fax: +49 89 442 49 831  
Email: [matthias.hofherr@atsec.com](mailto:matthias.hofherr@atsec.com)