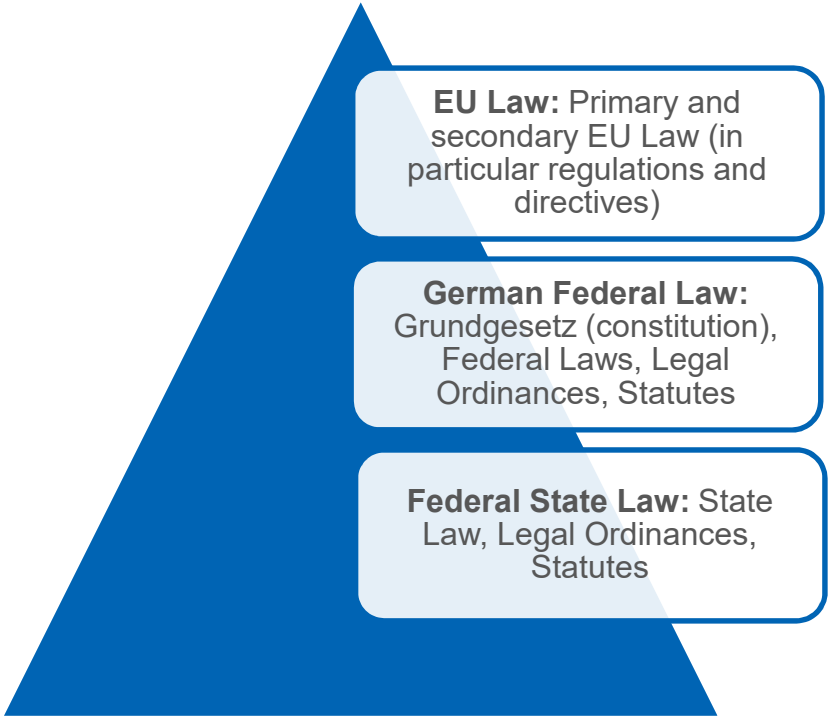
Legal Framework of IT Security in Germany and Europe

Dr. Dennis-Kenji Kipker
Legal Advisor
CERT@VDE

DKE
VDE DIN

German and European Regulatory Framework for Cybersecurity



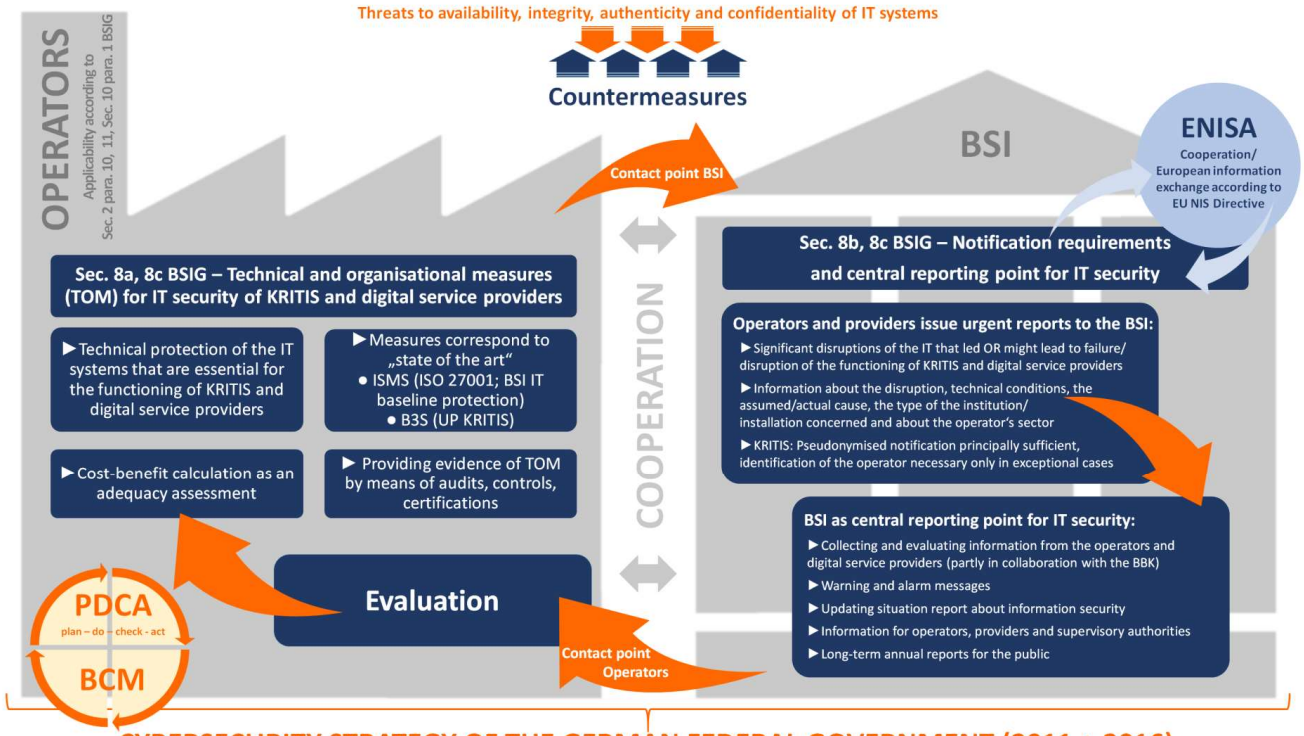
- **EU Network and Information Security Directive** (2016)
- **EU Data Protection Regulation GDPR** (2016, 2018, containing special data security regulations as well, Art. 32, in the case of affected personal data)
- **EU Cybersecurity Regulation („Act", CSA)** (2019)
  - Protection of the digital single interior market of the EU as main regulatory goal, consumer protection, facilitation of market access and compliance thoughout the whole EU
- **EU Regulation for a European Cybersecurity Competence Network and Centre** (draft, 2018)

- **1st IT Security Law of Germany** (2015)
  - BSI KRITIS Regulation (2016, 2017)
- **2nd IT Security Law of Germany** (draft, 2019 + 2020)
- **2nd Implementing Data Protection Law** (2019, changes German BSI Law, including extended use of personal data for reasons of IT security)

DKE
VDE DIN

Dr. Dennis-Kenji Kipker
IGMR
University of Bremen

INFORMATION FLOWS AND PROTECTION PROCESSES IN THE IT SECURITY OF CRITICAL INFRASTRUCTURES AND DIGITAL SERVICE PROVIDERS



CYBERSECURITY STRATEGY OF THE GERMAN FEDERAL GOVERNMENT (2011 + 2016)

(BSIG amended with specific regulations such as Sec. 109 TKG, Sec. 11 EnWG, Sec. 44b AtG; Opening clause in Sec. 8d para. 2 no. 5, para. 3 no. 5 BSIG, e. g. for health telematics)

IT Security Certification according to EU Cybersecurity Act

Assurance levels correspond to the level of the risk associated with the intended use of the ICT product, service or process, the probability and impact of an incident

“Rolling work programme” of EU COM defines list of relevant ICT products/services

In case of a certification (or statement of conformity after self-assessment), supplementary cybersecurity information has to be made publicly available by the manufacturer/provider in electronic form

Basic: Assures that the ICT product, service and process meets the corresponding security requirements and that they have been evaluated at a level intended to minimize the known basic risks of incidents and cyberattacks

Substantial: Assures that the ICT product, service and process meets the corresponding security requirements and that they have been evaluated at a level intended to minimize the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources

High: Assures that the ICT product, service and process meets the corresponding security requirements and that they have been evaluated at a level intended to minimize the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources

DKE
VDE DIN

2nd IT Security Law of Germany (draft, 2020)

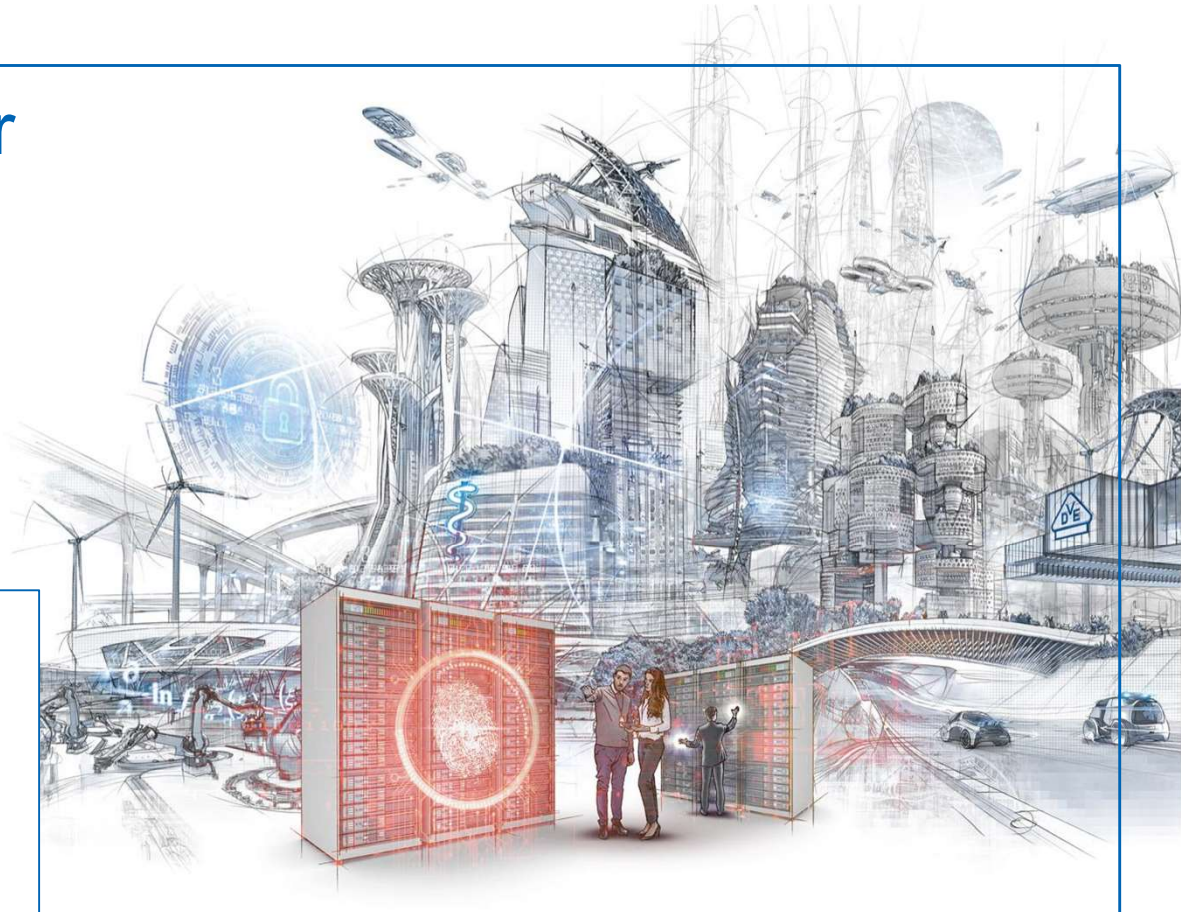
- **Main intention:** Further development of cybersecurity for the society as a whole
- Not only protection of Critical Infrastructures, but for all relevant companies and the state, as well as for consumers, **including IoT products**
- Co-regulation of EU Cybersecurity Act and German IT Security Law 2.0 in certain fields of interest
- **Core elements of the new regulatory approach include:**
  - Protection of citizens: Unified IT security mark, so that a higher visibility for IT security can be reached especially for consumer products/applications
  - Extensions of the legal power of the German BSI, as well as for criminal prosecution authorities to fight against cybercrime
  - New cybersecurity duties especially for providers, e.g. concerning the deletion, reporting, and the provision of information regarding cybercrime issues
  - More and effective cooperation among authorities to deal with cybercrime
  - Amended regulations for operators of Critical Infrastructures and important companies
  - Canceled: Extensions in the German Criminal Code and the German Criminal Prosecution Code

Impact of the current IT Security Legislation for Businesses and Consumers

- **Businesses:**
  - New resources have to be developed to be compliant with the upcoming cybersecurity regulation in Germany and Europe
  - Consumer trust is one of the key elements of EU cyber politics in the next years
  - Certifications will be valid in all EU Member States, which is supposed to make certification efforts more manageable for manufacturers
  - Certificates can be used for marketing purposes

- **Consumers:**
  - Consumers can choose between products knowing their security level
  - The certification thereby will allow consumers the valuation of security efforts and enable them to make informed choices
  - Transparency as one of the key requirements for future products and services
  - (Informed) self determination of the end user not only with regard to data protection, but IT security as well

Thank You for Your Attention!



Dr. Dennis-Kenji Kipker
Legal Advisor, CERT@VDE

Tel. +49 151 40223163
dennis-kenji.kipker@vde.com