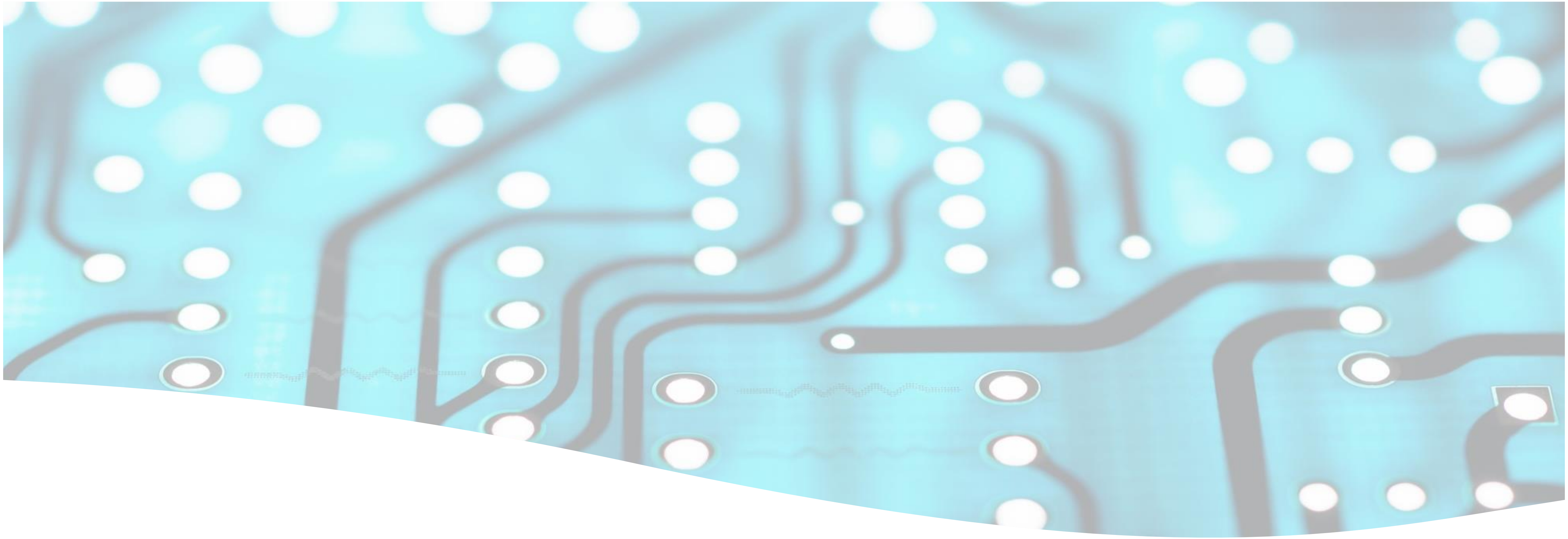


Cybersecurity Standards and Best Practices: Part 2 - Utilities and ISO/IEC 27001

Best Practices – Examples and Certified Utilities

USAID
FROM THE AMERICAN PEOPLE

USEA
United States Energy Association

EU NIS Directive

The Directive on Security of Information Systems (NIS-Directive) was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016. Member States had to transpose the Directive into their national laws by 9 May 2018 and identify operators of essential services by 9 November 2018.

Main Content:

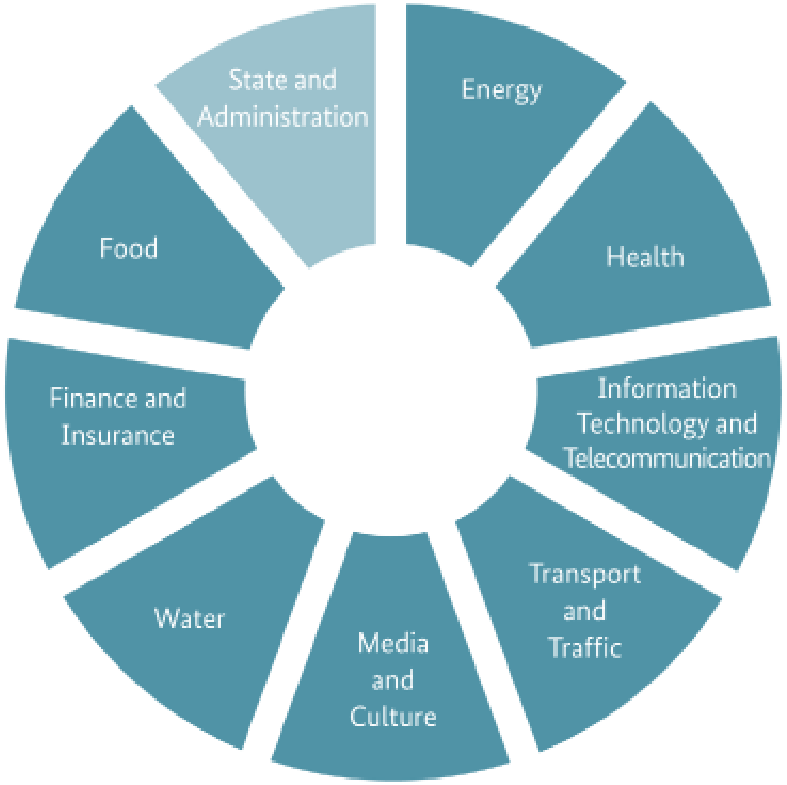
- Member States' preparedness on possible Cyber Attacks (e.g. by CSIRT setup)
- Strong Cooperation in between the member states on all topics of security and the consequent sharing of information on incidents and risks
- appropriate security measures for all identified Operators of essential services (OES) to gain a minimum baseline level of security allover the EU
- Key digital service providers (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the new Directive

NIS Implementation in Germany

A „real-life“ example from a energy grid provider perspective

NIS in Germany - Critical Infrastructures

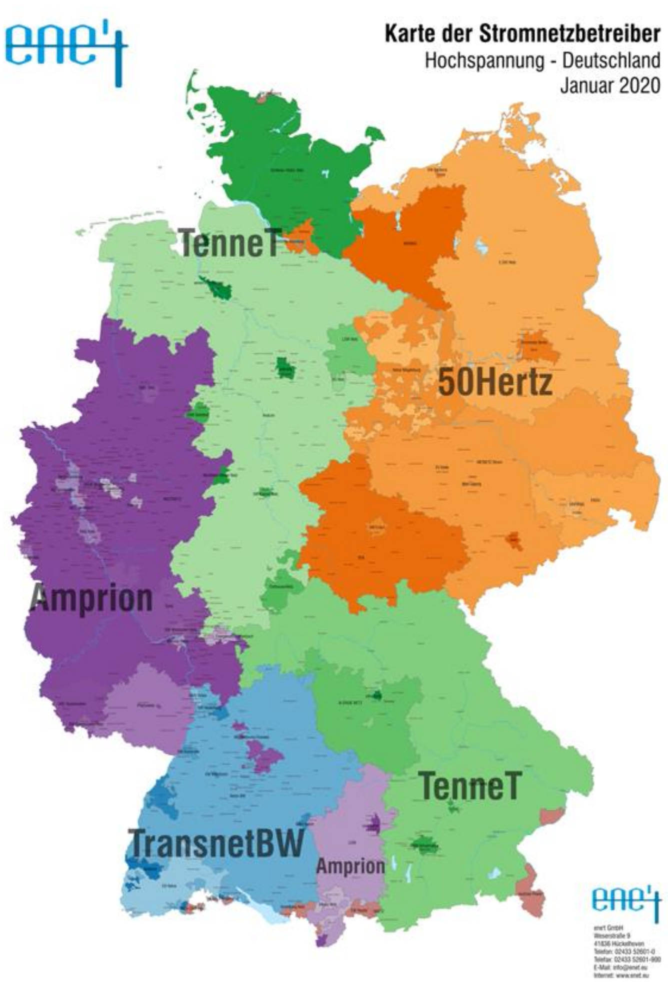
- All Operators of essential services are identified by the ministry of internal affairs, based on the KRITIS-Verordnung that contains the definitions and thresholds



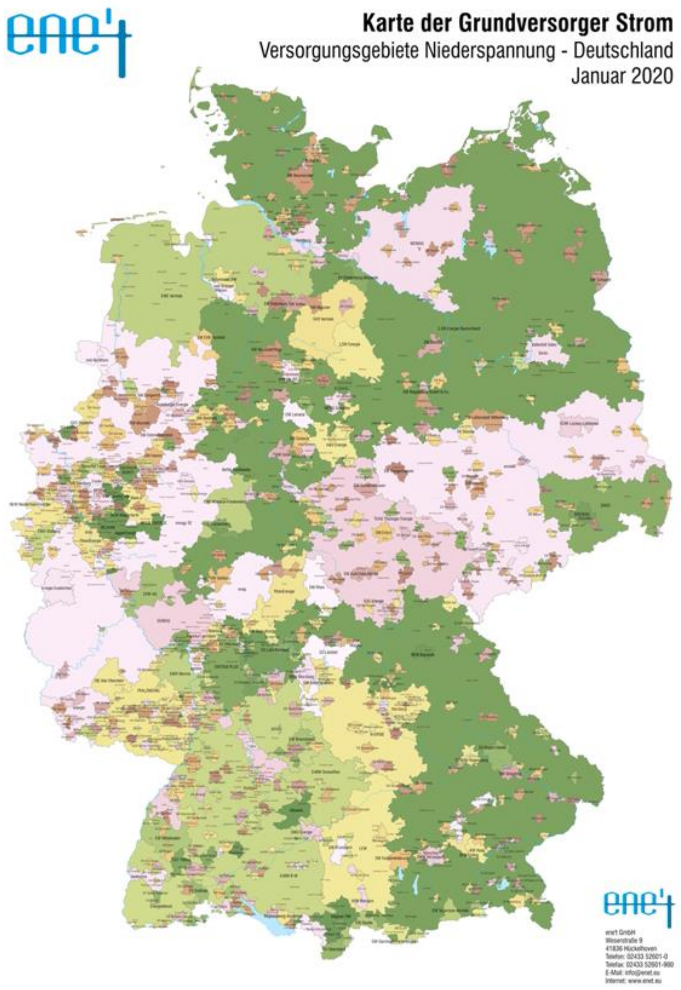
#	category	calculation criteria	threshold
1.2	Power transmission		
1.2.1	Transmission grid	Annual energy withdrawn by end consumers and distributors in GWh/year	3 700
1.2.2	Central system for electricity trading, related to physical short-term spot trading and the German market area	Exchange trading volume TWh/year	200
1.3	Power distribution		
1.3.1	Distribution grid	Annual energy withdrawn by end consumers and distributors in GWh/year	3 700
1.3.2	**Meter**	**Power of the connected consumption point or feed-in in MW**	420

All OES are required to comply to a minimum baseline of IT security

TSOs/DSO landscape in Germany



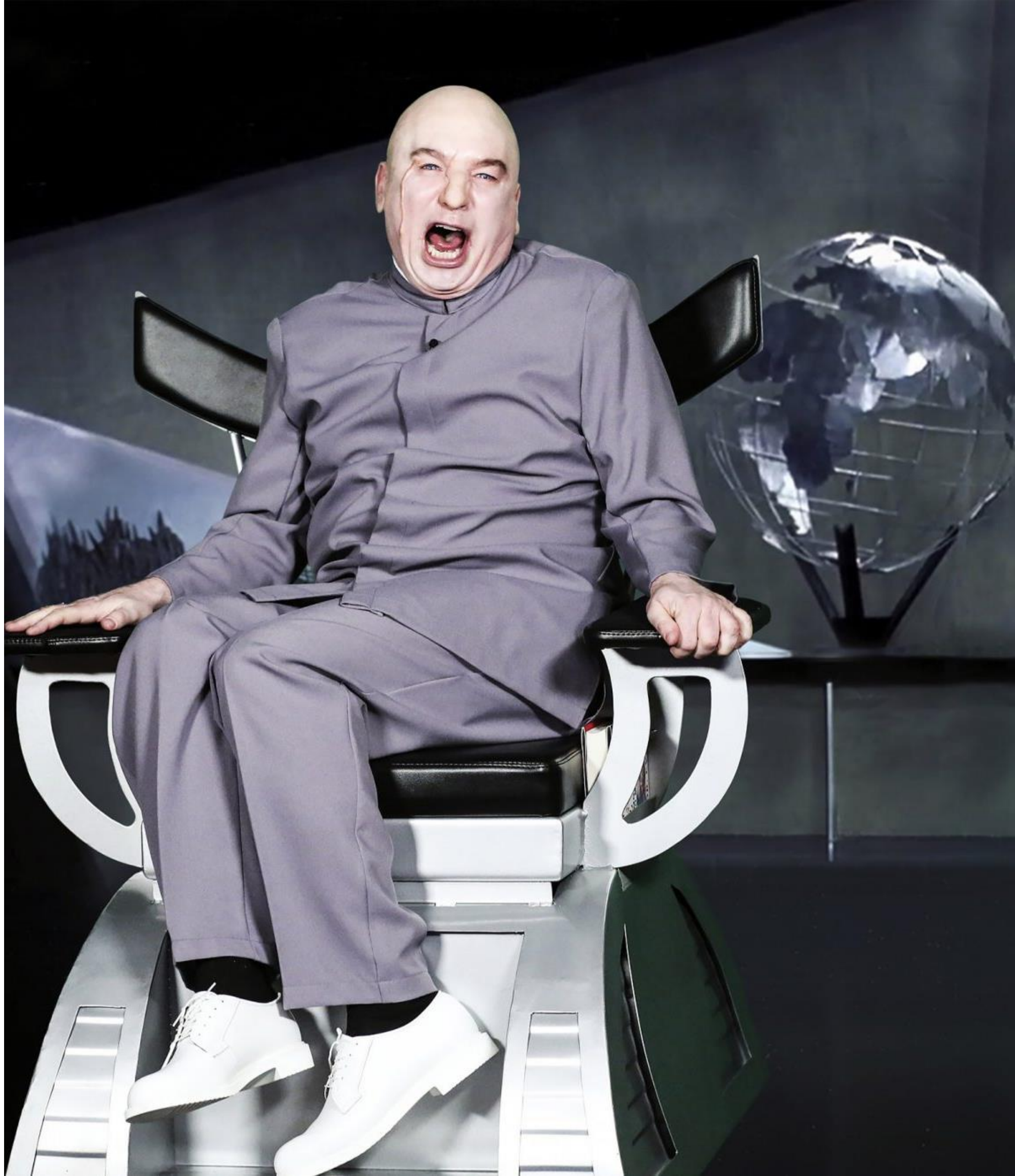
4 large TSOs


enet
Karte der Grundversorger Strom
Versorgungsgebiete Niederspannung - Deutschland
Januar 2020
enet

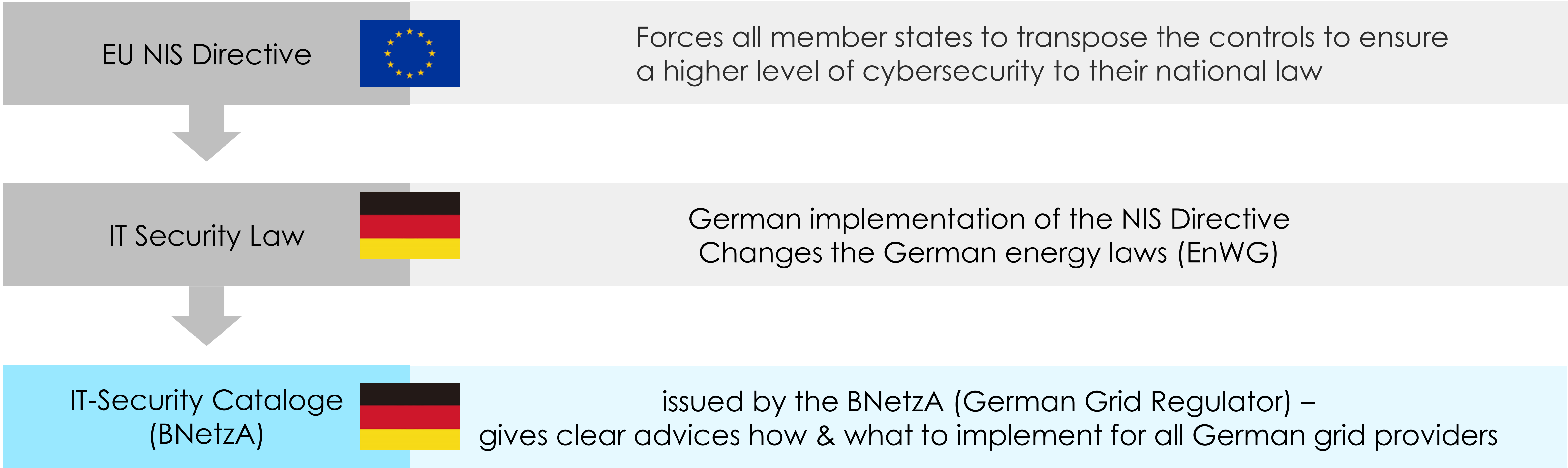
890 DSOs & 726 gas grid providers (all sizes)

→ **All of them were identified as OES! (undepending from size/area)!!**

How can you assure, that all those different OES are complying to a minimum baseline of IT security ??



Regulations in Germany



EU NIS Directive

Forces all member states to transpose the controls to ensure a higher level of cybersecurity to their national law

IT Security Law

German implementation of the NIS Directive
Changes the German energy laws (EnWG)

IT-Security Cataloge (BNetzA)

issued by the BNetzA (German Grid Regulator) –
gives clear advices how & what to implement for all German grid providers

Lets have a closer Look-
What´s in the IT – Security catalog?

Only 16 pages – but a high effect for German energy grid providers (both, TSO and DSO)!

✓ Every TSO/DSO has to nominate a contact point/contact person for IT Security, that can provide information regarding incidents that occurred and the current status of the implementation of security measures in cooperation with the authorities at any time.

✓ Every TSO/DSO has to send a structured grid plan with all relevant components to the regulator

✓ Every TSO/DSO has to be ISO/IEC 27001 and ISO/IEC 27019 (Information security controls for the energy utility industry) certified and regularly re-certified

Questions!

- Should utilities have an integrated approach or should they reduce the scope to the bare minimum?
- Which version of standards should a utility select?
- What does the certification process look like?
- What are the benefits of certification?

Should utilities have an integrated approach or should they reduce the scope to the bare minimum?

- TSOs/DSOs in Germany didn´t have a choice – the scope was defined by the regulator

Scope: All central and decentral components, that are nesseccary for the secure operation of the grid

- **BUT:** the benefit of a full-scope approach is pretty clear!
- The risk based approach of the ISO/IEC 27001 helps to focus on the really critical processes in the first step
- The Continual Improvement is an important part of the standard and helps to increase the maturity of the whole management system step-by-step
- Are you really able to exclude some parts of your company from the scope because they are “not important”?

Which version of standards should a utility select?

- The answer is easy – always the newest (with a transition period) ;)
- In ISO/IEC standards are reviewed at least every 3 years and can be confirmed unchanged, revised or reviewed by the experts. A revision of a standard takes about 3-4 years until publication [ISO/IEC 27001:2013 was confirmed in 2018]

For utility industries the **ISO/IEC 27019:2013 [Information security controls for the energy utility industry]** is extremely helpful, because it gives additional guidance on grid components like e.g. legacy systems and can be used in combination with ISO/IEC 27001

ISO/IEC 27019 – specialized on energy utilities

- While legacy systems don´t play a role in ISO/IEC 27001 because they are normally not part of the IT infrastructure – ISO/IEC 27019 gives guidance on those “OT specials”

10.11.1 Treatment of legacy systems Control
All conventional legacy process control system technologies, systems and components (hereinafter referred to as legacy systems) should be identified along with their potential information security vulnerabilities. Appropriate controls should be implemented in order to mitigate all of the identified risks associated with such legacy systems.

Implementation guidance
A large number of the process control systems used in the energy utility industry are based on legacy technologies which lack basic security features. To provide an appropriate level of security, the risks resulting from continued use of legacy systems and technologies should be identified. In situations where standard controls cannot be implemented, other types of countermeasure should be applied, for example:

a) The implementation of strict and appropriate network segregation.

b) Remote access for configuration and maintenance purposes should be avoided. If remote access is absolutely necessary, proper network isolation, e.g. through the use of secure proxy services should be ensured. Access for maintenance purposes should only be provided via defined interconnection points that are operated and monitored securely.

c) Strict access control rules should be enforced at the network, system and application levels.

d) It should be ensured that only state of the art equipment and components are used for maintenance and configuration purposes.

ISO/IEC 27019 – specialized on energy utilities

- Also the password requirements for OT systems are slightly different…

Energy utility-specific implementation guidance

- In the process control domain it is not always possible to ensure the use of secure passwords, e.g.:
- legacy systems often do not allow for individual passwords and/or passwords with necessary strength;
- It is frequently impossible to connect systems operated at decentralized plants, such as substations or distributed generation units, to central directory services, which means that local accounts and passwords have to be used. This makes it practically impossible to change passwords regularly.
- It should therefore be clearly indicated to the user when the general password policy applies and where different passwords are to be used or where it is not possible to use any passwords at all (legacy systems).
- Especially in situations where only one unique password is used for general system access, the password should be chosen to be as secure as possible. In particular, the standard passwords used by the system vendors should be considered as insecure and widely known. Passwords should only be accessible to persons who are involved in the operation of the system.

What does an audit look like?

oh oh!

Auditor ≠ Auditor

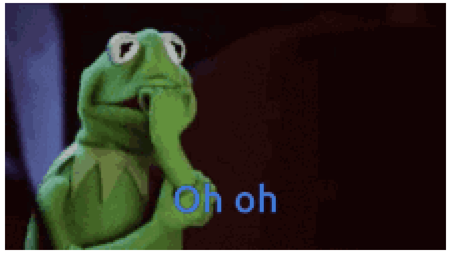
- Publication of the conformity assessment program for the accreditation of certification bodies for the IT security catalog on April 13, 2016 by the BSI based on ISO / IEC 27006

- The certification scheme was created through the collaboration between the Federal Network Agency and the BSI

- The following points are defined by the accreditation scheme:

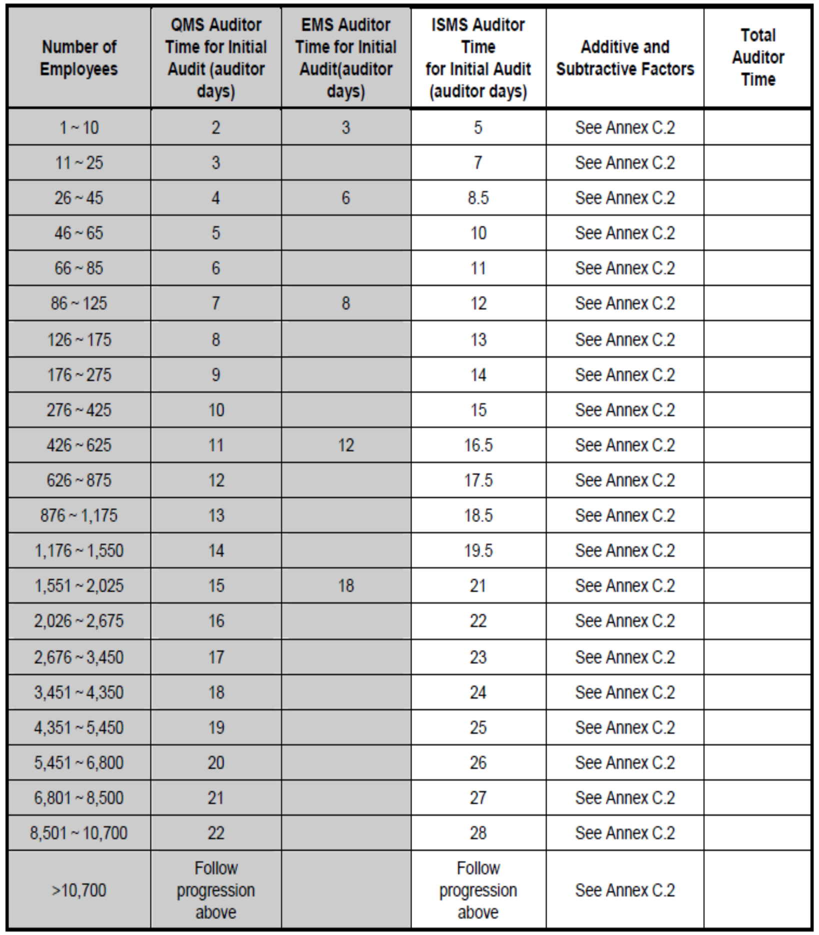
  - Auditors have to undergo training on the fundamentals of grid-based energy supply with electricity and gas

  - To check the scope and the risk analysis according to the IT security catalog, the audit team must call in a specialist (studies + at least three years of relevant professional experience in grid-based energy supply)

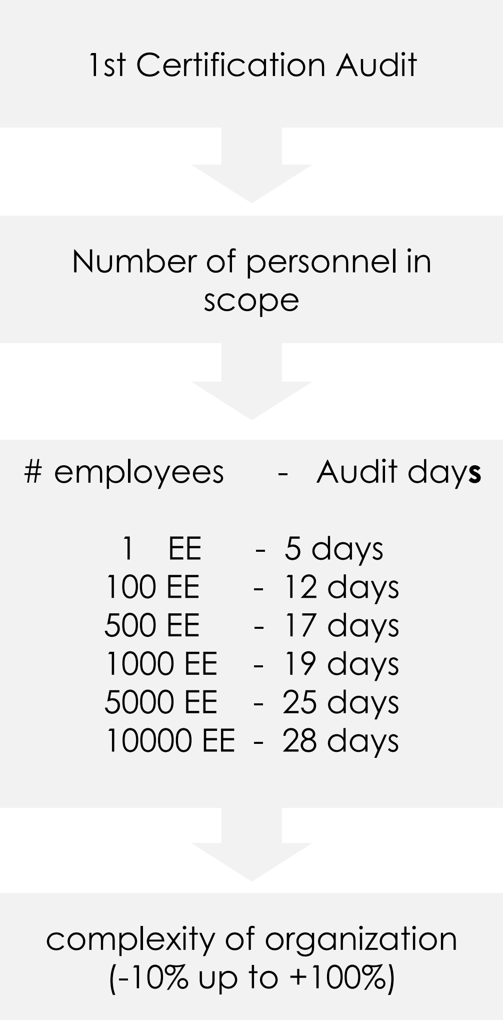


Calculation of Audit time

- Based on ISO/IEC 27006



Number of Employees	QMS Auditor Time for Initial Audit (auditor days)	EMS Auditor Time for Initial Audit(auditor days)	ISMS Auditor Time for Initial Audit (auditor days)	Additive and Subtractive Factors	Total Auditor Time
1 ~ 10	2	3	5	See Annex C.2	
11 ~ 25	3		7	See Annex C.2	
26 ~ 45	4	6	8.5	See Annex C.2	
46 ~ 65	5		10	See Annex C.2	
66 ~ 85	6		11	See Annex C.2	
86 ~ 125	7	8	12	See Annex C.2	
126 ~ 175	8		13	See Annex C.2	
176 ~ 275	9		14	See Annex C.2	
276 ~ 425	10		15	See Annex C.2	
426 ~ 625	11	12	16.5	See Annex C.2	
626 ~ 875	12		17.5	See Annex C.2	
876 ~ 1,175	13		18.5	See Annex C.2	
1,176 ~ 1,550	14		19.5	See Annex C.2	
1,551 ~ 2,025	15	18	21	See Annex C.2	
2,026 ~ 2,675	16		22	See Annex C.2	
2,676 ~ 3,450	17		23	See Annex C.2	
3,451 ~ 4,350	18		24	See Annex C.2	
4,351 ~ 5,450	19		25	See Annex C.2	
5,451 ~ 6,800	20		26	See Annex C.2	
6,801 ~ 8,500	21		27	See Annex C.2	
8,501 ~ 10,700	22		28	See Annex C.2	
>10,700	Follow progression above		Follow progression above	See Annex C.2	



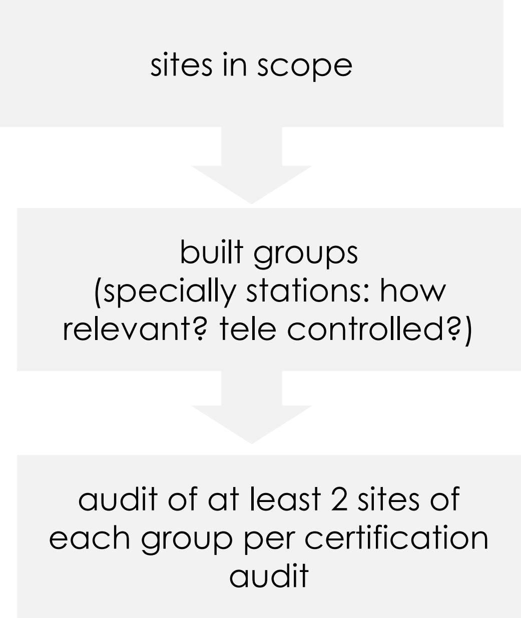
1st Certification Audit

Number of personnel in scope

# employees - Audit days

1 EE - 5 days
100 EE - 12 days
500 EE - 17 days
1000 EE - 19 days
5000 EE - 25 days
10000 EE - 28 days

complexity of organization
(-10% up to +100%)



sites in scope

built groups
(specially stations: how relevant? tele controlled?)

audit of at least 2 sites of each group per certification audit

But - What are the benefits of ISO/IEC 27001?

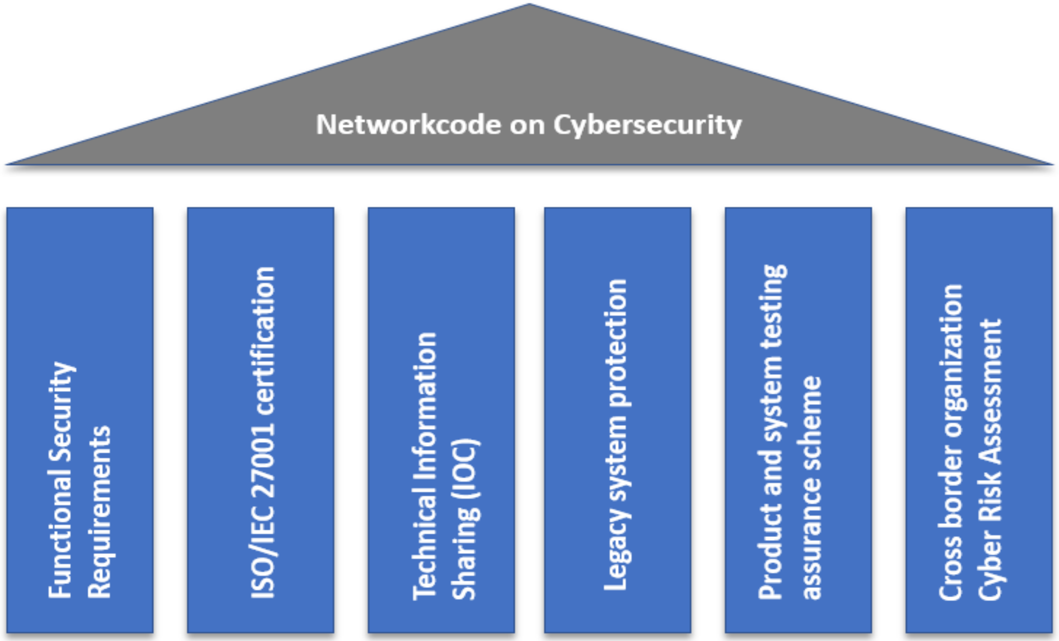
- Mandatory ISMS certification helps to raise management attention and therefor also the budget for cybersecurity
- Level of security is raised permanently due to the continual improvement
- Overall security management system approach includes **all parts of the business**, not only special security measures (including e.g. personell, awareness …)
- Security becomes part of the companies DNA – acceptance is raised significantly
- Fast reaction on new threats and vulnarabilities – as result of the risk based approach
- Flexible management system that can be easily adopted even after changes within the company
- Additional standards give guidance on special systems enviroments (no – ISO/IEC 27001 is NOT an IT only standard)

What are the benefits of the certification?

- Minimum Baseline Level of Security of all german gas and electricity grid providers is achieved
- The similar scope for the certification makes all providers compareable
- Certificate can be used to fullfily security requirements within the supply chain (e.g. TSOs except certificate of DSOs as evidence that baseline security is achieved without performing extra time and cost intensive audits like they did in the past)
- The yearly survailence audits garantee that a continual improvemnet takes place and that all findings are delt with

The way forward…

- The European Commission announced the set-up of a cybersecurity working group in spring 2017 based on the "Clean Energy for all Europeans' (COM/2016/0860 final) package.
- The group delivered a report end of 2018 with the clear advice to setup a network code on Cybersecurity
- Network codes are binding EU documents for all European TSOs and DSOs


Networkcode on Cybersecurity

Functional Security Requirements

ISO/IEC 27001 certification

Technical Information Sharing (IOC)

Legacy system protection

Product and system testing assurance scheme

Cross border organization Cyber Risk Assessment

Backup

Infos

ISO/IEC 27001 – Leadership Responsibilities

5.1 Leadership and commitment
Top management shall demonstrate leadership and commitment with respect to the information security management system by:

a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;

b) ensuring the integration of the information security management system requirements into the organization’s processes;

c) ensuring that the resources needed for the information security management system are available;

d) communicating the importance of effective information security management and of conforming to the information security management system requirements;

e) ensuring that the information security management system achieves its intended outcome(s);

f) directing and supporting persons to contribute to the effectiveness of the information security management system;

g) promoting continual improvement; and

h) supporting other relevant management

IT Sicherheitskatalog BNetzA (EnWG §11,1a)

- Link

it_sicherheitskatalog_bnetza.pdf