

National Implementation of Cyber Security Requirements

Walter Wutzl, Digital Grid Automation Products
September 12-13, 2019 | VAR Partner Day 2019 | Bled, Slovenia

National Implementation of Cyber Security Requirements

The Directive on Security of Network and Information Systems (NIS Directive)

- Entered into force in August 2016.
- Deadline for implementation for member states was November 2018
 - Implementation in Austria started with December 2018 ...
- Most of our customers are affected
 - Operators of Essential Services




Intensive activities regarding cyber security with Austrian utilities since 2013

- Due to a communication problem that affected almost all utilities in May 2013
- Multiple workshops/ research projects with utilities and universities
- Developing strategies and technical solutions



Starting of discussions with Austrian Operational NIS Authority in the Ministry of Internal Affairs

 Bundesministerium
Inneres

Implementation of the NIS Directive in Austria...

...from the point of view of the Operational NIS
Authority in the Ministry of Internal Affairs

Overview

- **NIS Directive**
 - EU Directive on security of network and information systems
- Cybersecurity Act
 - EU legal act on cyber security
- NIS-Law & NIS-Regulation
 - Implementation of NIS Directive into Austrian law

NIS Directive

- **Background**
 - IT systems play a central role in society
 - Reliability and security are crucial to economic and social activities and the proper functioning of the internal market
- **Directive (EU) 2016/1148 of 6th July 2016**
 - Directive on measures to ensure a high common level on security of network and information systems in the European Union
 - 1. legal act on cybersecurity in the EU

Overview

- NIS Directive
 - EU Directive on security of network and information systems
- **Cybersecurity Act**
 - EU legal act on cyber security
- NIS-Law & NIS-Regulation
 - Implementation of NIS Directive into Austrian law

Cybersecurity Act

- **Permanent mandate** for the European Union Agency for Network and Information Security (**ENISA**) with increased funding
- Among other things, ENISA will serve as an independent **center of competence** and should also contribute to **capacity building** within the EU
- Establish an EU-wide **European certification framework** for cybersecurity of **products, processes and services**
- The framework should consider security characteristics such as **"Security by Design"**

Overview

- NIS Directive
 - EU Directive on security of network and information systems
- Cybersecurity Act
 - EU legal act on cyber security
- **NIS-Law & NIS-Regulation**
 - Implementation of NIS Directive into Austrian law

NIS-Law – Objectives and Goals

- Establish measures to achieve a high level of security of network and information systems
 - In particular by:
 - National strategy for the security of network and information systems
 - Establishment of national organizational and coordination structures
 - **Security requirements and reporting requirements**
 - Tasks and requirements for computer emergency teams
 - Data protection
 - **Sanctions**

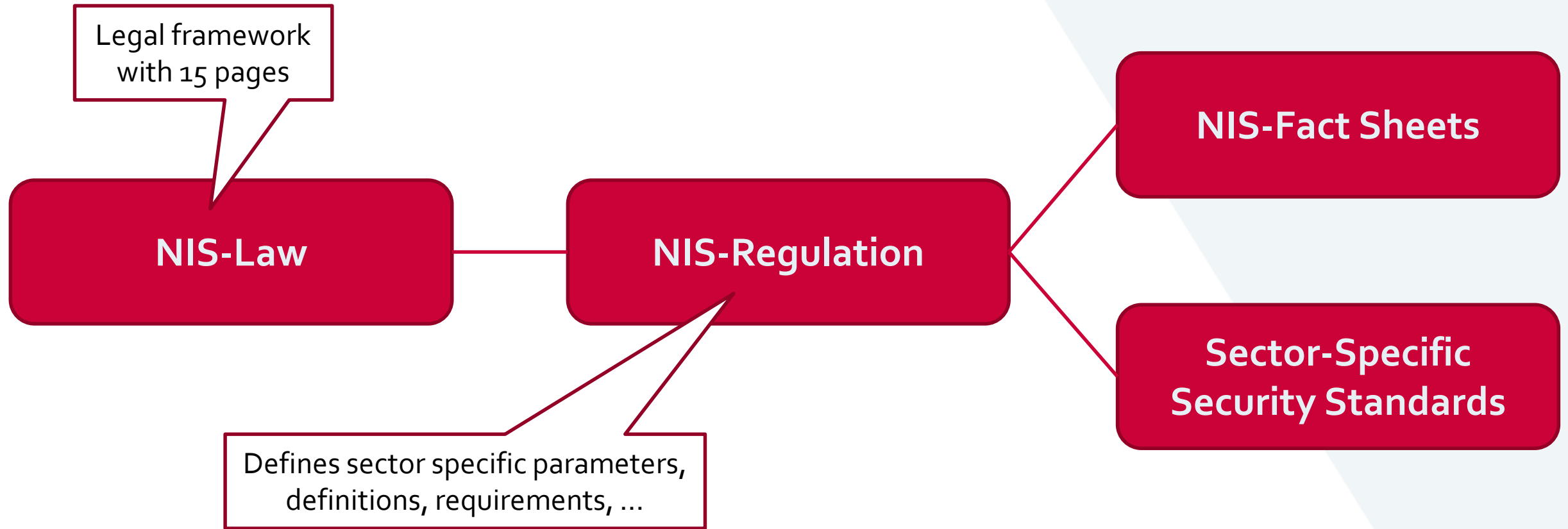
Adressees

- Addressees of the NIS-Law are
 - Providers of digital services
 - **Operators of essential services**
 - Public administration facilities
- Addressees are essential for the proper functioning of the community
- Obligations
 - Taking security precautions
 - Reporting security incidents
- Computer emergency teams / Qualified Bodies

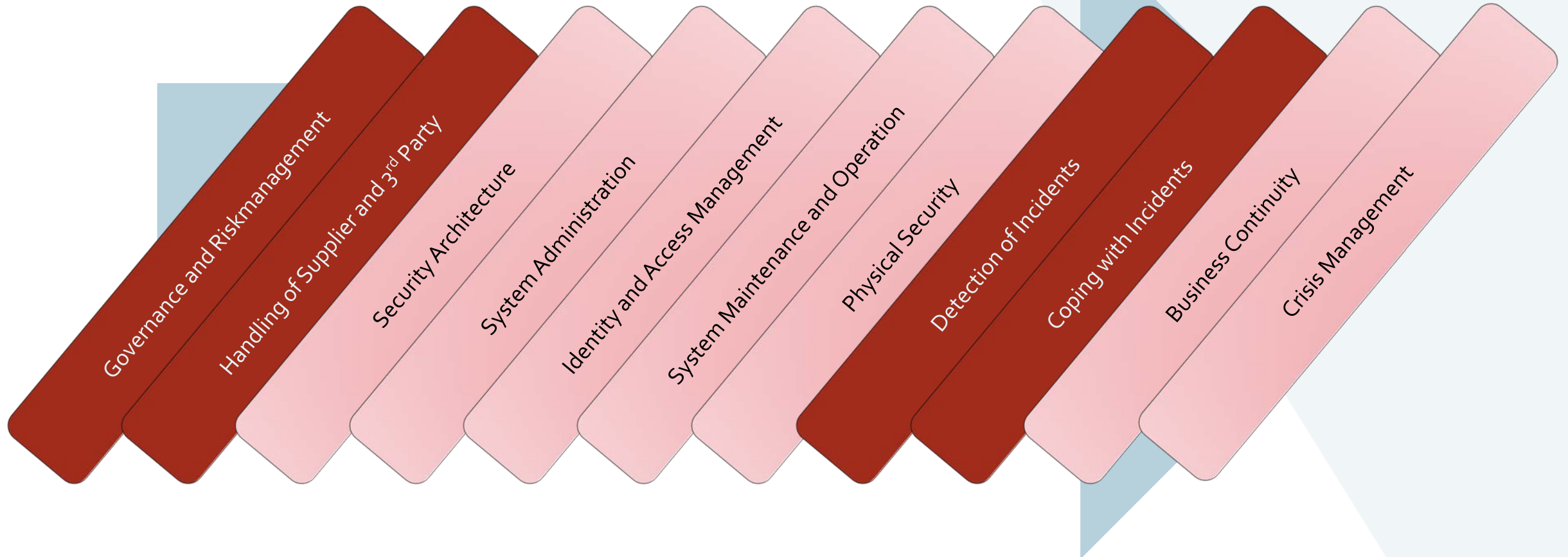
Operators of Essential Services

- The Office of the Federal Chancellor determines
 - for each sector, those operators with a branch in Austria,
 - **who provide an essential service**
1. Energy
 2. Transport
 3. Banking sector
 4. Financial market infrastructure
 5. Healthcare
 6. Drinking water supply
 7. Digital infrastructure

Security Measures – Framework



Security Measures for Operators of Essential Services



NIS Fact Sheet 08/2018

- NIS Fact Sheet 08/2018 – Mapping table, example:

2.2.1 Governance und Ökosystem

#	Kategorie	Sicherheits- maßnahme	Ö. Informations- sicherheits- handbuch Version 4.0.1	BSI IT- Grundschutz ⁵	ISO 27001:2013	ISA/IEC 62443 3-3	CIS CSC Version 6.0	CIS CSC Version 7.0	NIST CYBER SECURITY FRAMEWOR K
1	Governance und Risikomanageme nt	Risikoanalyse	4 Risikoanalyse	<i>BSI-Standard 100-2, Kapitel 3, 4, 5, BSI- Standard 100-3, Risikoanalyse auf der Basis von IT- Grundschutz</i>	8.2 Information security risk assessment 8.3 Information security risk treatment	SR 5.1, 5.2, 5.3	1, 2, 4, 13, 14, 17	1, 2, 3, 13, 14, 17	ID.GV-4 ID.RA- 1,2,3,4,5,6 D.RM-1,2,3 PR.AT-2

Check Cycle of Security Measures for Operators of Essential Services by Qualified Bodies

Audit reports of
qualified bodies
(„partial verification
possibility“)

In general: proof of
requirements
Every 3 years

Implementation of Security Requirements Products, Solutions and Services

Products

- Security for control centers
- Security for embedded systems
- Security for engineering tools



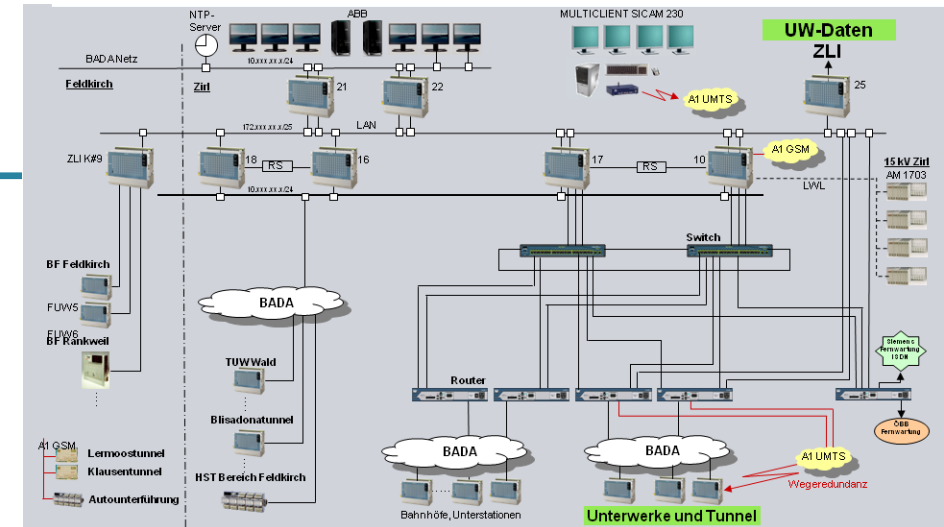
System

- Network segmentation
- Data transmission via unsecured networks
- Back up / Restore
- Patch management
- Integration / upgrade of existing systems



Human

- Security Know How
- Security Maintenance



Implementation of Security Requirements by Defined Process

Technical Assessment

- Of existing system

Assessment of Technical Risks

- Based on ISO 27001 requirements

Definition of Measures for the Security Enhancement

- Based on [bdew Whitepaper](#) and ISO 27001/ ISO 27019



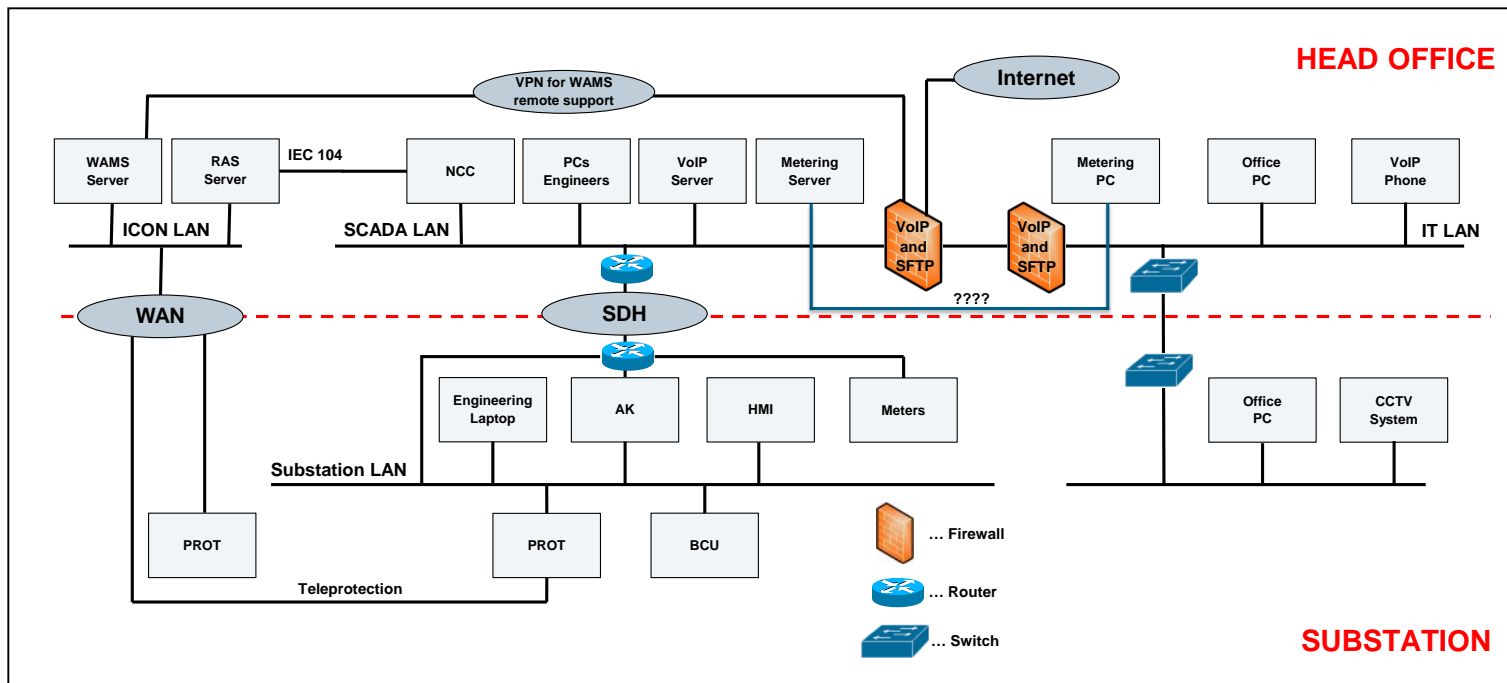
[Link to BDEW](#)



Implementation of Security Requirements by Defined Process

Technical Assessment

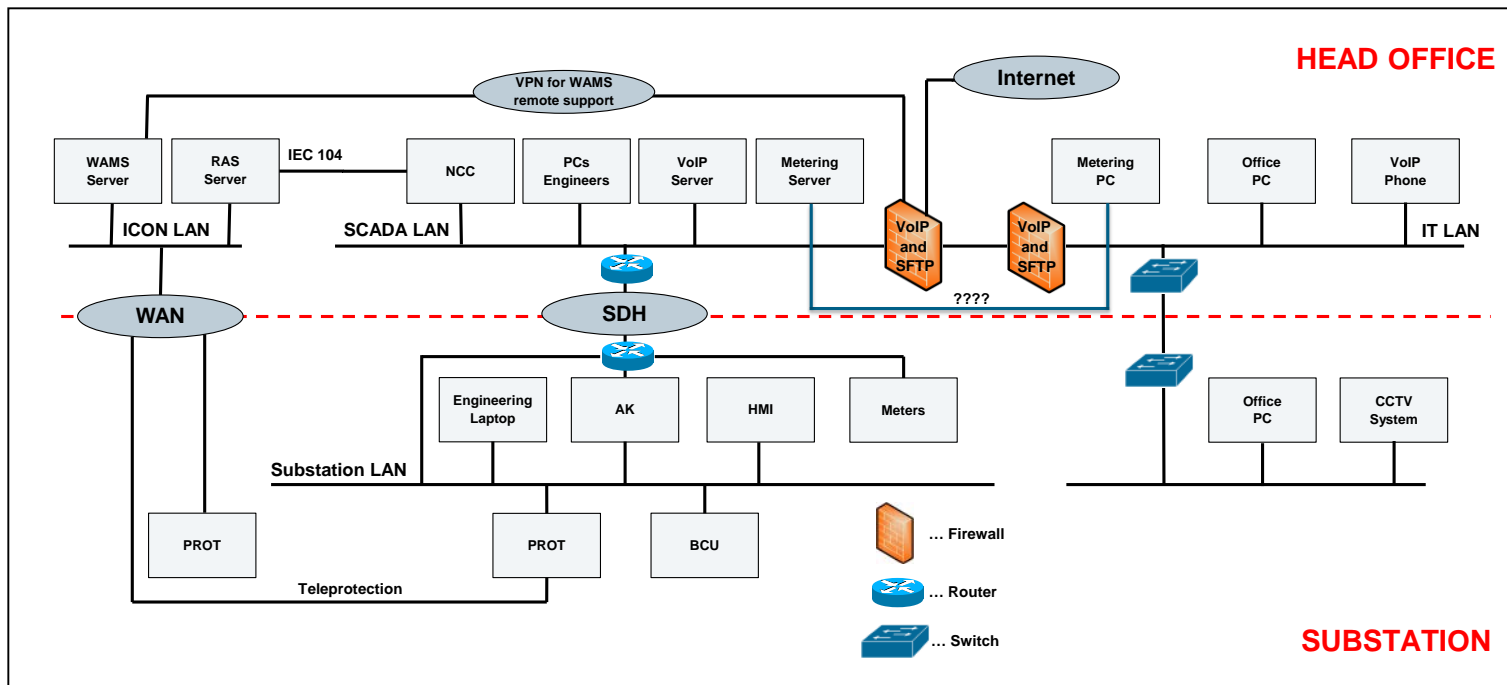
- Of existing system



Implementation of Security Requirements by Defined Process

Assessment of Technical Risks

- Based on ISO 27001 requirements



	Very Likely	Acceptable Risk (medium - 2)	Unacceptable Risk (high - 3)	Unacceptable Risk (extreme - 5)
	Likely	Acceptable Risk (low - 1)	Acceptable Risk (medium - 2)	Unacceptable Risk (high - 3)
	Unlikely	Acceptable Risk (low - 1)	Acceptable Risk (low - 1)	Acceptable Risk (medium - 2)
Occurrence / Impact		Low	Moderate	High

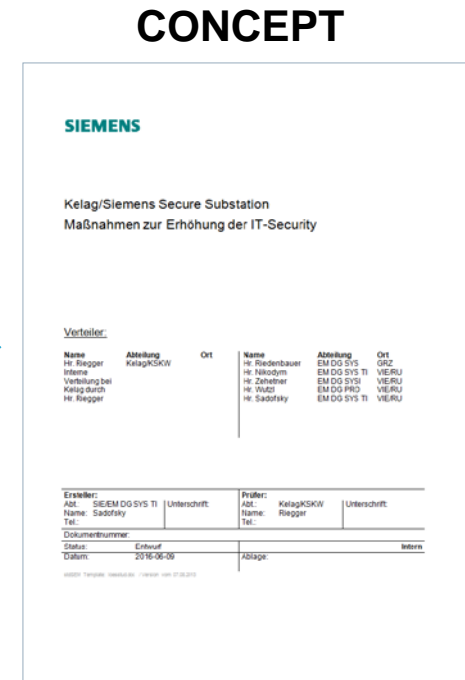
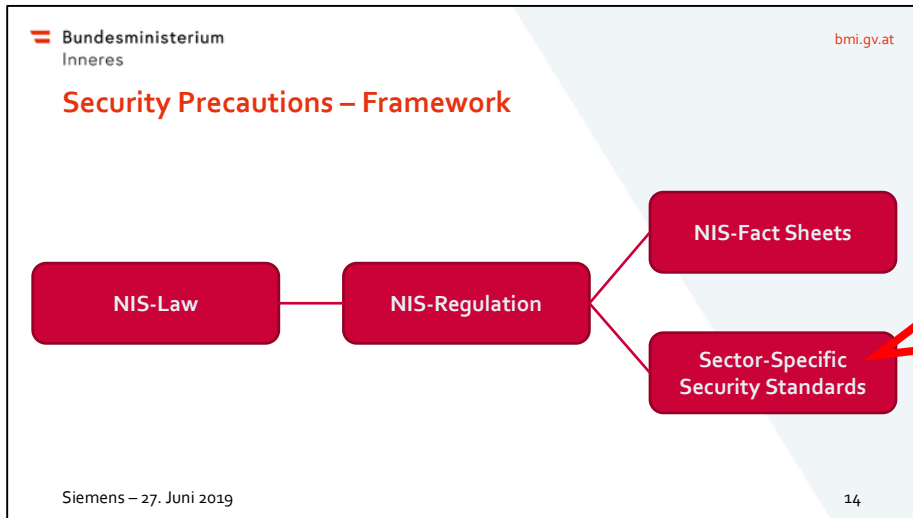
Probability x Impact = Risk

Impact (how serious is the risk?)

Implementation of Security Requirements by Defined Process

Definition of Measures for the Security Enhancement

- Based on bdeu Whitepaper and ISO 27001/ ISO 27019
- Definition of target state
 - Resulting necessary measures
 - Including specific generic blueprints
 - Considering organizational setup



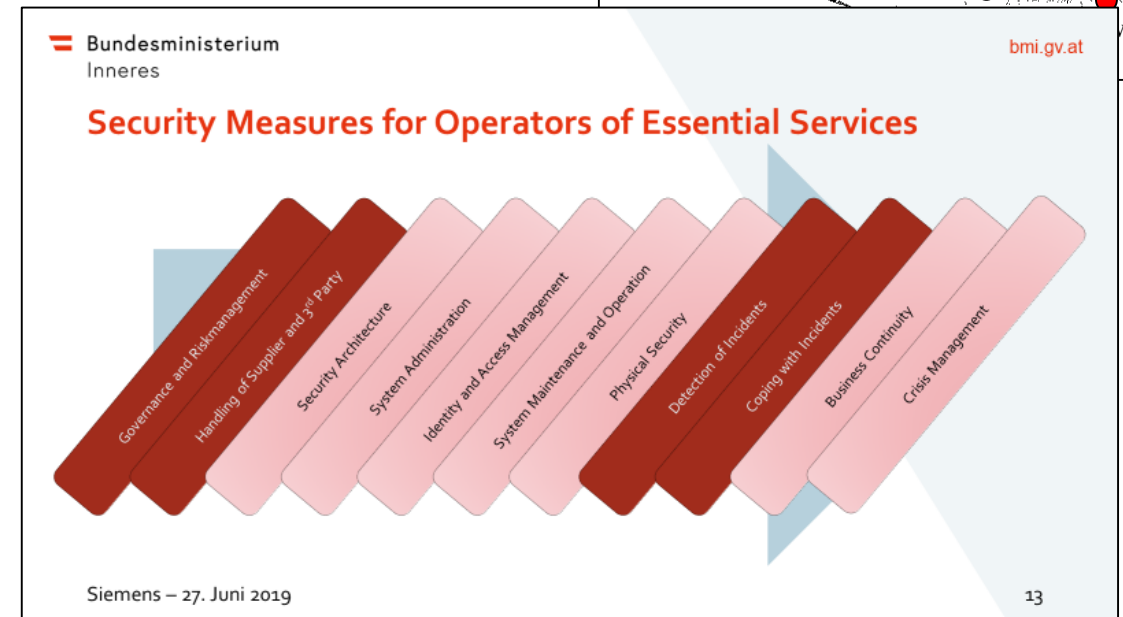
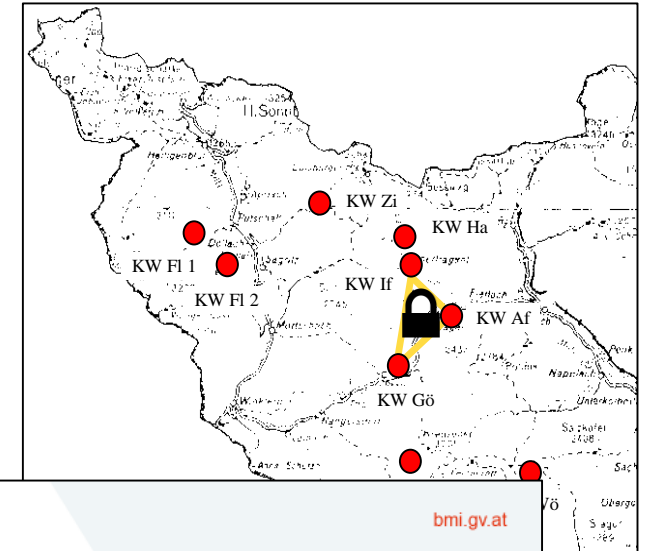
Implementation of Security Requirements First Project in 2015

Improvement of Security of Installed Base

- Systematic analyses/ expansion of already implemented security measures
- Maintain compatibility with existing systems
- With reasonable efforts for both parties

Implementation of Recommendations and Measures According to

- bdew-Whitepaper
- ISO 27001 (ISO 27002 + ISO 27019)



Thank you for your attention!

SIEMENS
Ingenuity for life



Walter Wutzl
Head of Digital Grid Products

Siemens Smart Infrastructure / Digital Grid
Siemensstrasse 90
A-1210 Vienna

Tel: +43 5 1707 -31587

E-Mail: walter.wutzl@siemens.com

[siemens.at/var](https://www.siemens.at/var)