NTS

RELAX, WE CARE

NIS 2.0
NETZ- UND INFORMATIONSSYSTEMSICHERHEIT

21.06.2023 | ADV E-Government Konferenz, Graz

KONTAKTDATEN

ROMAN A. TOBLER
Senior Manager | Technology Risk

ERNST & YOUNG MANAGEMENT CONSULTING GMBH
Wagramer Straße 19, IZD Tower, 1220 Wien, Austria
T: +43 1 / 211 70 4392
Mail: roman.tobler@at.ey.com

ALEXANDER MÜLLNER
Territory Manager

NTS NETZWERK TELEKOM SERVICE AG
Trabrennstraße 2b, 1020 Wien, Austria
T: +43 1 / 876 67 76 – 413, F: – 56
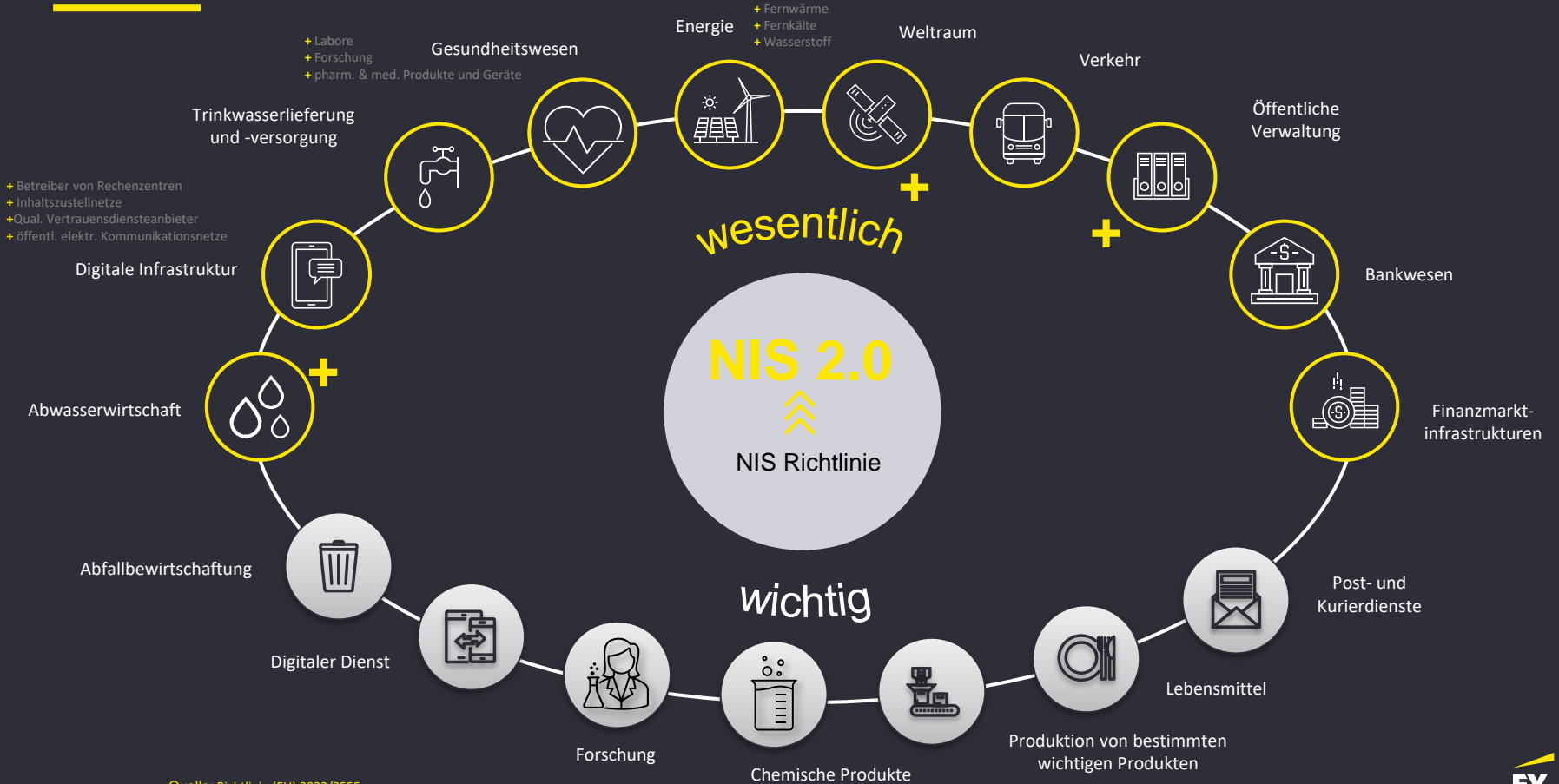M: +43 664 / 88 239 413
Mail: alexander.muellner@nts.eu

Stufenbau der Rechtsordnung

EU

AT

NIS2 RL
Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (Richtlinie (EU) 2022/2555)

NISG
Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz (BGBl. I Nr. 111/2018)

VO
Nationale Verordnungen zur Ausführung des NISG, wie NISV (BGBl. II Nr. 215/2019), QuaSteV (BGBl. II Nr. 226/2019)

BS
Branchenstandards zur Festlegung sektorspezifischer Vorkehrungen. Genehmigung durch BMI
bspw: Elektrizitäts-Sektor (AT-3SV-Elektrizität), Sektor Wasser-DE (B3S-Wasser)

14.12.2022

17.10.2024
„Sie (MS) wenden diese Vorschriften ab dem 18. Oktober 2024 an."

EY

Welche Unternehmen/Sektoren sind von der NIS 2.0 betroffen?
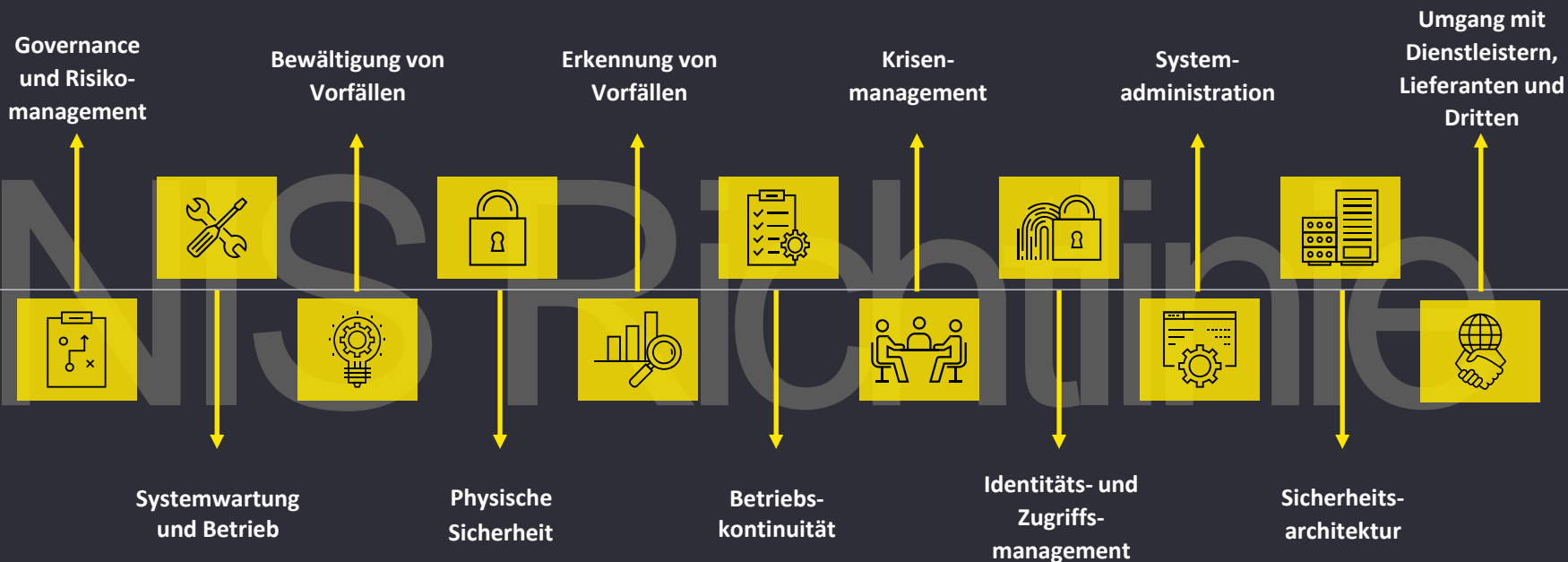
Gesundheitswesen
+ Labore
+ Forschung
+ pharm. & med. Produkte und Geräte

Energie
+ Fernwärme
+ Fernkälte
+ Wasserstoff

Weltraum

Verkehr

Trinkwasserlieferung und -versorgung

Öffentliche Verwaltung

Digitale Infrastruktur
+ Betreiber von Rechenzentren
+ Inhaltszustellnetze
+ Qual. Vertrauensdiensteanbieter
+ öffentl. elektr. Kommunikationsnetze

Bankwesen

Abwasserwirtschaft

Finanzmarktinfrastrukturen

Abfallbewirtschaftung

Post- und Kurierdienste

Digitaler Dienst

Lebensmittel

Forschung

Chemische Produkte

Produktion von bestimmten wichtigen Produkten

wesentlich

wichtig

NIS 2.0
NIS Richtlinie

Quelle: Richtlinie (EU) 2022/2555

EY

NIS2 Directive – Network and Information Security Directive

Article 21 NIS2

Entities must take operational and organizational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimize the impact of incidents on recipients of their services and on other services.

Measures shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following Risk management measures:

Diagram: central node "Risk management measures" connected to:
- Internal Risk analysis policies
- Incident Handling
- Business Continuity
- Supply Chain Security
- Security in network and information systems acquisition
- Cybersecurity policies and effectiveness assessment
- Cyber Hygiene Practices
- Cryptography and Encryption
- HR Security
- Multi Factor Authentication

EY

INFORMATIONS-SICHERHEIT

Informationssicherheit
macht glücklich,
wenn man rechtzeitig
d'rauf schaut,
daß man's hat,
wenn man's braucht:

NTS RELAX, WE CARE

EY Building a better working world