sila consulting
be compliant

NIS 2
Von der gesetzlichen Anforderung in die praktische Umsetzung

sila consulting GmbH
part of netgo group GmbH

Vorstellung

sila consulting
be compliant

EU NIS-2 Cybersecurity | Überblick

Wo

- NIS2-Umsetzungsgesetz (NIS2UmsuCG ??)
- Teil der KRITIS-Regulierung
- NIS-2-Richtlinie (27.12.2022)

Wann

- Als nationales Gesetz in Kraft: **geplant 2. Hj 2025**
- Nachweisprüfungen:
  - Für besonders wichtige Unternehmen **2** Jahre nach Veröffentlichung

Wer

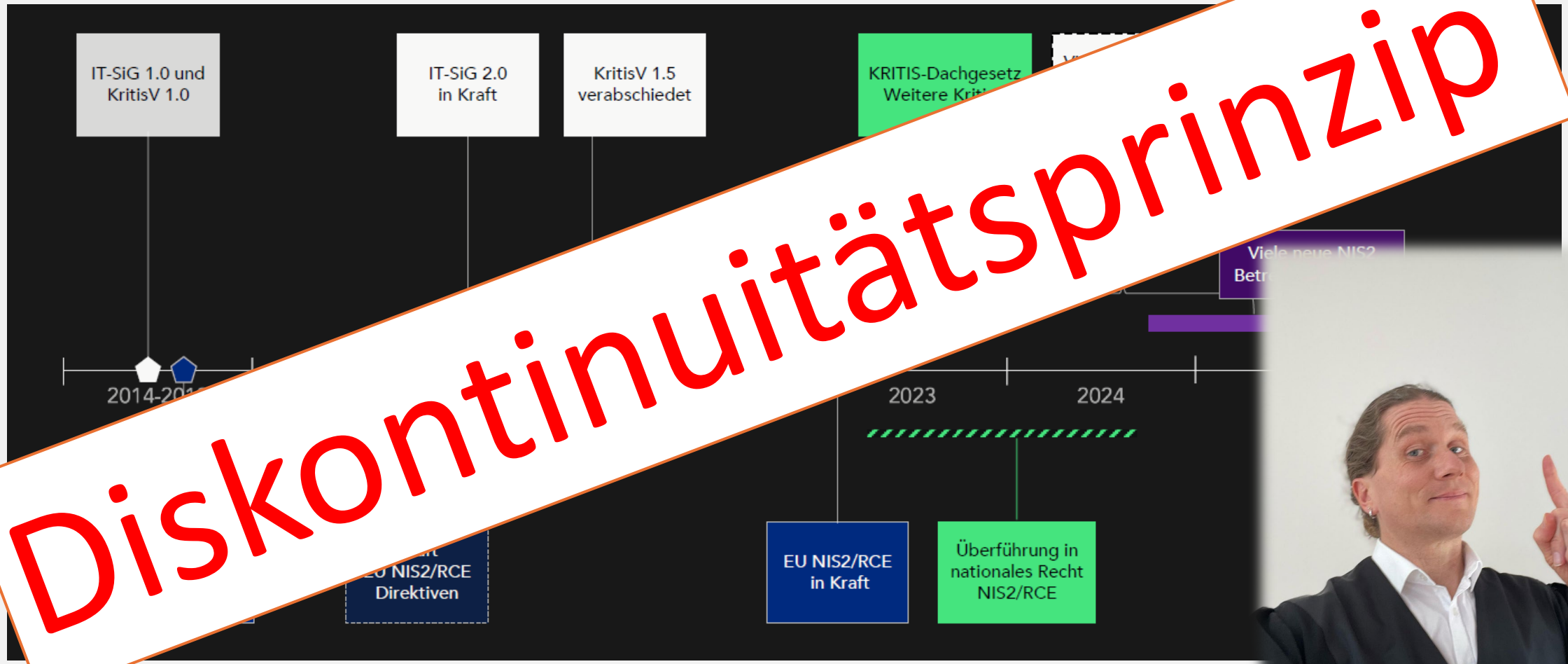
- Umsetzung:
  - Besonders wichtige / Wichtige Unternehmen
- Kontrolle:
  - SPOC in Deutschland ist das BSI

Was

- In Kürze: ISMS wird zum „must-have“
- umfangreiche Maßnahmen zur Stärkung der Cyber-Resilienz
- Konzepte zur Risikoanalyse
- BCM / Krisenmanagement

- Meldepflichten für Vorfälle
- Registrierungspflicht

NIS-2 im Zeitstrahl



Diskontinuitätsprinzip

Was bedeutet das Diskontinuitätsprinzip (O-Ton Thorsten Stelter)?

Für den Bundestag gilt das Diskontinuitätsprinzip. Es beinhaltet die **sachliche, personelle und organisatorische** Diskontinuität (**Nicht-Fortsetzung**) nach Ablauf einer Wahlperiode.

- **Sachliche Diskontinuität:** Alle Gesetzesvorlagen, die vom alten Bundestag noch nicht beschlossen wurden, müssen neu eingebracht und verhandelt werden.
- **Personelle Diskontinuität:** Alle bisherigen Abgeordneten verlieren mit der Konstituierung eines neu gewählten Bundestages ihr Mandat.
- **Organische Diskontinuität:** Alle Untergliederungen und Organe des Bundestages wie etwa die Ausschüsse müssen neu gebildet werden

Der Grundsatz leitet sich teils aus dem Grundgesetz (Art. 39 GG), teils aus der Staatspraxis und die in § 125 der Geschäftsordnung des Bundestages geregelt ist.

Grundgedanke hinter diesem Prinzip:

- **Sicherung der demokratischen Legitimation**
- **Verhinderung von Altlasten früherer Parlamente**
- **Jedes Parlament soll eigenständig entscheiden können.**

Was bedeutet das für NIS2?

- **Sachliche Diskontinuität:** Alle Gesetzesvorlagen, die vom alten Bundestag noch nicht beschlossen wurden, müssen neu eingebracht und verhandelt werden.

Quelle:BMI - Gesetzgebungsverfahren - Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

EU NIS-2 Cybersecurity | Betroffene

Nach Unternehmensgröße

Klein

- ✓ weniger als 50 Mitarbeiter
- ✓ weniger als 10m EUR Umsatz

Betrifft nur **besonders** kritische Anbieter.

Mittel

- ✓ 50 – 249 Mitarbeiter
  oder
- ✓ 10 – 50 m EUR Umsatz
- ✓ oder bis 43m Jahresbilanz

Groß

- ✓ ab 250 Mitarbeiter **oder**
- ✓ mehr als 50m EUR Umsatz
- ✓ oder mehr als 43m Jahresbilanz

Aus 18 Sektoren

Annex I (Essential)

- Energie
- Transport
- Bankwesen
- Finanzmarkt
- Gesundheit
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- ICT Service Management
- Öffentliche Verwaltung
- Weltraum

Annex II (Important)

- Post & Kurier
- Abfall
- Chemikalien
- Lebensmittel
- Herstellung
- Digitale Dienste
- Forschung

EU NIS-2 | Aufgaben & Pflichten

Risikomanagementmaßnahmen

- Geltungsbereich definieren
- Backup- & Krisenmanagement
- Management und Offenlegung von Schwachstellen
- Schulungen zur Cybersicherheit
- (weitere) Technische & methodische Anforderungen können noch erlassen werden
- Langfristig ggf. Einführung von Cybersicherheitszertifizierungen für IKT-Produkte/Dienste/Prozesse
- Informationsaustausch zwischen Dienstleistern über Portal des BSI

Ohne Gewähr

Meldepflichten

- Stufenweise Meldung (**24h**, 72h, …) zur Lage eines erheblichen Sicherheitsvorfalls
  - Ausführliche Beschreibung: Art der Bedrohung, Ursache, getroffene Maßnahmen, Auswirkungen
  - Empfänger der Dienste informieren, um Maßnahmen zur Bedrohungsabwehr einzuleiten

Registrierungspflicht

- Kontaktdaten, E-Mail-Adresse, IP-Adressbereiche, Telefonnummern, …
- BSI legt Verfahren noch genauer fest

Nachweispflichten

- Generell für besonders wichtige Einrichtungen
- alle 3 Jahre durch Audits / Zertifizierung für Betreiber kritischer Anlagen
- Mängelbeseitigung auf Verlangen des BSI

Hilfe, was soll ich tun?

Grundsätzlich z.B. §8a BSIG

Gesetzliche Anforderungen

Mappen auf

ISO

Bundesamt
für Sicherheit in der
Informationstechnik

Standards international/national/branchenspezifisch

Geben vor

erfüllen

Prüfungshilfe/Vorgaben

NIS 2 Mapping?

Gesetzliche Anforderungen

Mappen auf

ISO

Ohne Gewähr

Mapping ISO 27001 auf NIS2

NIS2UmsuCG	Anforderung	ISO 27001:2022
§30 (1) Satz 1	Maßnahmen basierend auf Risiko-Exposition und gesellschaftlichen und wirtschaftlichen Auswirkungen	4.3
		6.1
		8.2
		8.3
		A.5.4
		A.5.29
		A.5.30
§30 (1) Satz 3	Dokumentation der NIS2 Risiko-Management Maßnahmen	6.1.3
		8.3
		A.5.31
§30 (2) Satz 1	Allgefahrenansatz und Stand der Technik	6.1
		8.2
		8.3
		A.5.29
		A.5.30
§30 (2) Nr. 1	Konzepte zur Risiko-Analyse (IT-RM)	6.1
		8.2
		8.3
		10.1
		A.5.31
		A.5.36
		A.8.34
§30 (2) Nr. 1	Konzepte für IT-Sicherheit (ISMS)	4.1-10.2
		A.5.1
		A.5.2
		A.5.3
		A.5.4

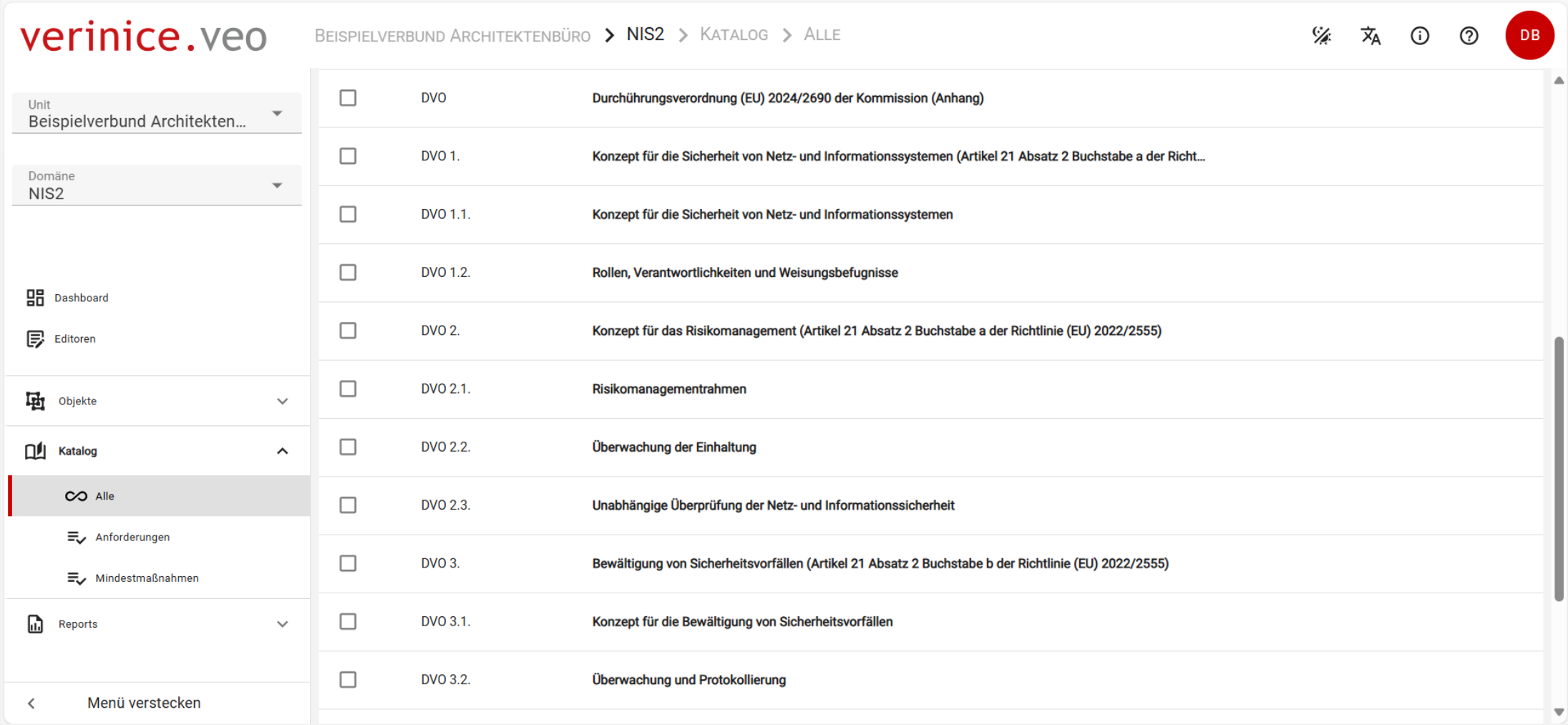
Quelle:
NIS2-Mapping auf KRITIS und ISO 27001 Cybersecurity – OpenKRITIS

Ohne Gewähr

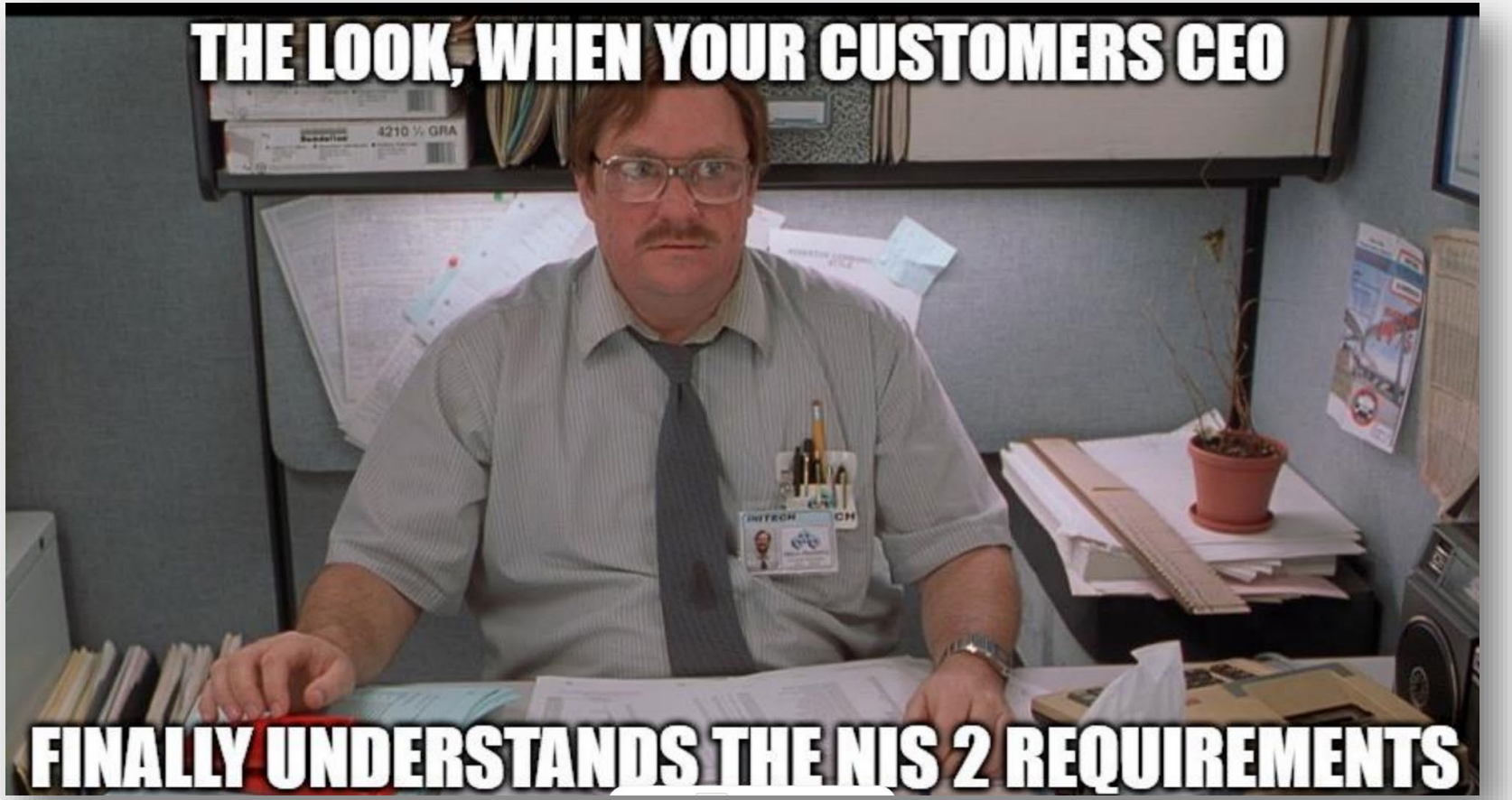
Pragmatisch

- Stellen Sie fest ob Sie „wichtiges“ oder „besonders wichtiges“ Unternehmen sind
- Registrieren Sie sich
- Implementieren Sie ein ISMS nach einem Standard (ISO/BSI).
  - Zertifikat -> **Houv niet, mag wel**
- Etablieren Sie Meldewege
  - Aufnahme als Stakeholder
  - Sicherheitsvorfallmanagement

Zum krönenden Abschluss



Final


THE LOOK, WHEN YOUR CUSTOMERS CEO
FINALLY UNDERSTANDS THE NIS 2 REQUIREMENTS

Fragen?

sila consulting
be compliant

Alle genutzten Grafiken und Fotos entstammen direkt Office 365 oder wurden von Mitarbeitern aus Unternehmen der netgo group bearbeitet. Es bestehen keine Rechtsansprüche Dritter.

sila consulting GmbH

Telefon: +49 2861 82549 -0

E-Mail: info@sila-consulting.de

www.sila-consulting.de

Danke fürs Zuhören!