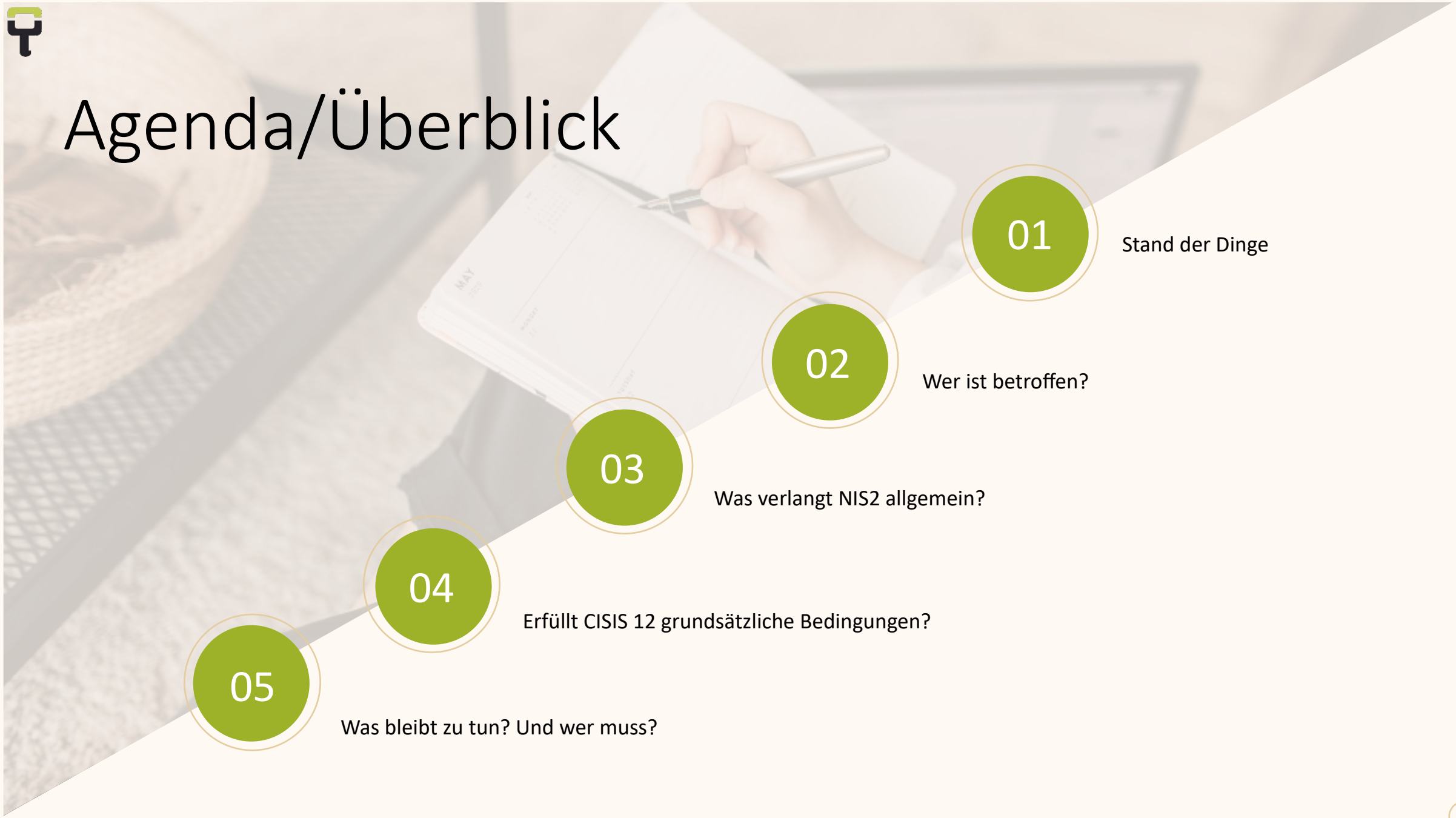
NIS2 und CISIS12?

IT-Sicherheitscluster e. V.

ITSECURITY

www.it-sicherheitscluster.de

Agenda/Überblick



01 Stand der Dinge

02 Wer ist betroffen?

03 Was verlangt NIS2 allgemein?

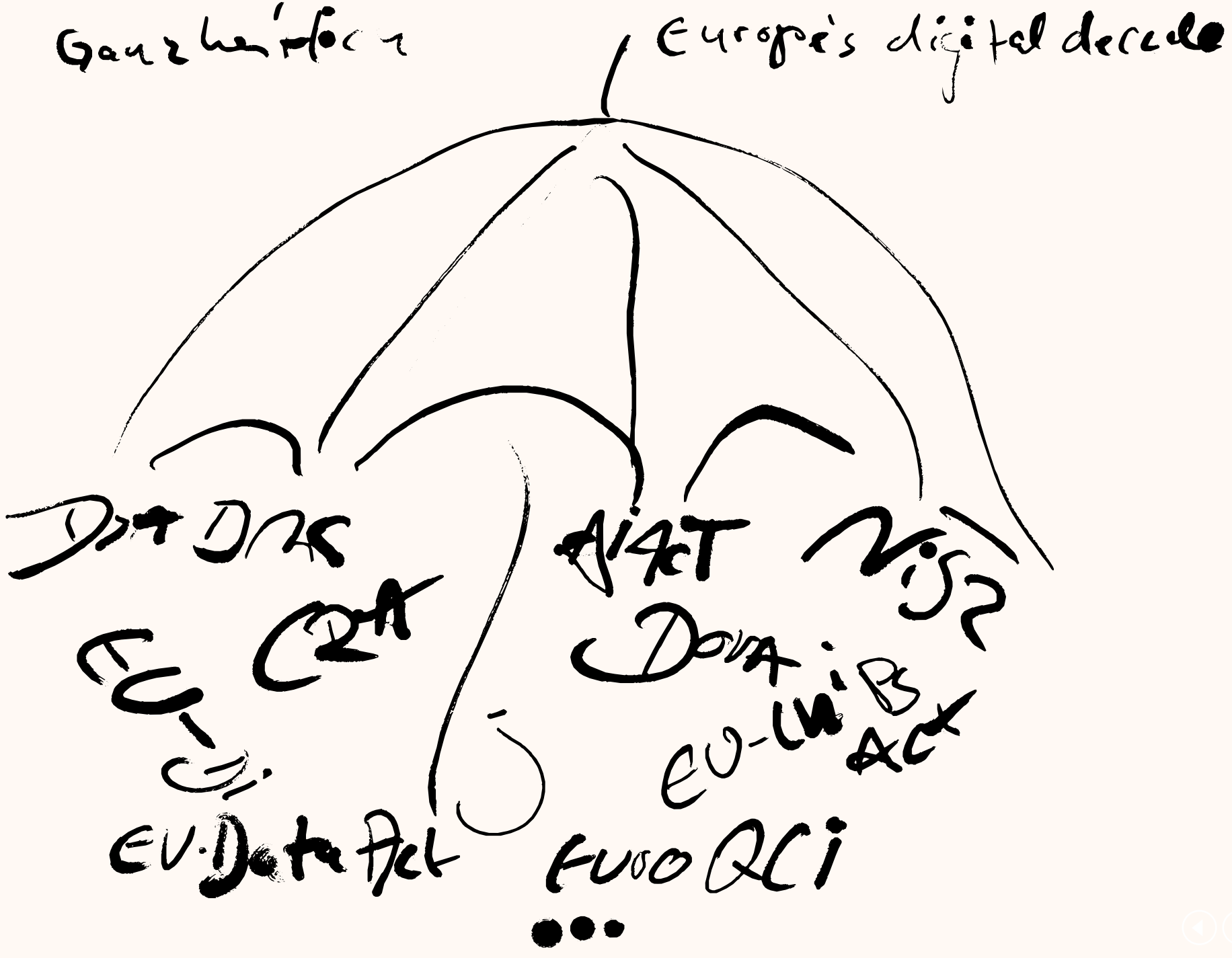
04 Erfüllt CISIS 12 grundsätzliche Bedingungen?

05 Was bleibt zu tun? Und wer muss?

Was ist NIS2? Stand der Dinge

Europa?

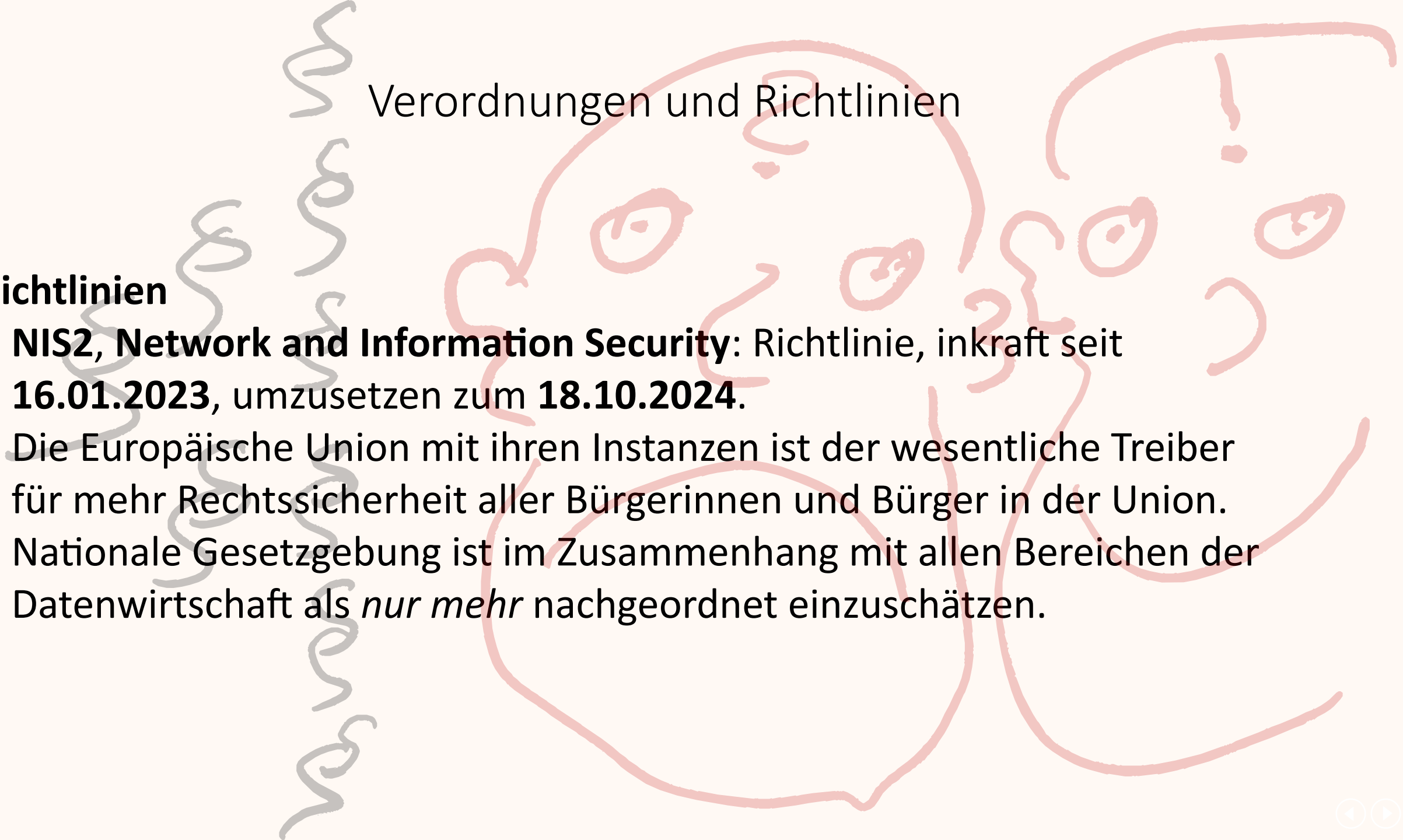
Wer steigt durch?



Wozu?

Was bringen die Regeln?

Verordnungen und Richtlinien



Richtlinien

- **NIS2**, **Network and Information Security**: Richtlinie, inkraft seit **16.01.2023**, umzusetzen zum **18.10.2024**.
- Die Europäische Union mit ihren Instanzen ist der wesentliche Treiber für mehr Rechtssicherheit aller Bürgerinnen und Bürger in der Union.
- Nationale Gesetzgebung ist im Zusammenhang mit allen Bereichen der Datenwirtschaft als *nur mehr* nachgeordnet einzuschätzen.

NIS2

- Aktualisierung von NIS (Network Information Security) von 2016.

- Ziel: Definition einheitlicher Standards für die Errichtung eines „hohe[n] gemeinsame[n] Cybersicherheitsniveau[s] in der Union. Höheres Sicherheitsniveau für kritische Infrastruktur.
- Leitender Grundsatz: Mindestharmonisierung.

Wer ist betroffen?

Wer ist betroffen?

- **Mittelständische Unternehmen** mit einer Größe von 50-250 Mitarbeitern und einem
- jährlichen Umsatz von 10-50 Mio. Euro bzw. einer Bilanzsumme von bis zu 43 Mio. Euro,
- **Großunternehmen** ab einer Größe von 250 Mitarbeitern mit einem Umsatz ≥ 50 Mio. EUR bzw. einer Bilanzsumme ab 43 Mio. EUR.
- Unabhängig von der Größe gilt die Richtlinie
  - für Einrichtungen der Sektoren aus Anhang I oder II,
  - Anbietern von öffentlichen elektronischen Kommunikationsnetzen oder
  - von öffentlich zugänglichen elektronischen Kommunikationsdiensten; Vertrauensdiensteanbietern,
  - Namenregistern der Domäne oberster Stufe und Domänennamensystem-Diensteanbietern.
  - Wenn es nur den **einzigen Anbieter eines Dienstes** gibt, der für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten unerlässlich ist;
  - der Dienstes **wesentlich auf die öffentliche Ordnung, die öffentliche Sicherheit oder die öffentliche Gesundheit auswirken könnte**;
  - eine **Störung** des von der Einrichtung erbrachten Dienstes zu einem **wesentlichen Systemrisiko** führt
  - Kritisch für andere Mitgliedsländer.
  - Verwaltung ist auch betroffen. Dabei geht es um risikobasierte Einordnung der Organisation.

Praktisches Ziel

Vermeidung von Störungen, die erhebliche Auswirkungen auf kritische und/oder gesellschaftliche und/oder wirtschaftliche Tätigkeiten haben.

Betroffene Sektoren

Hohe Kritikalität

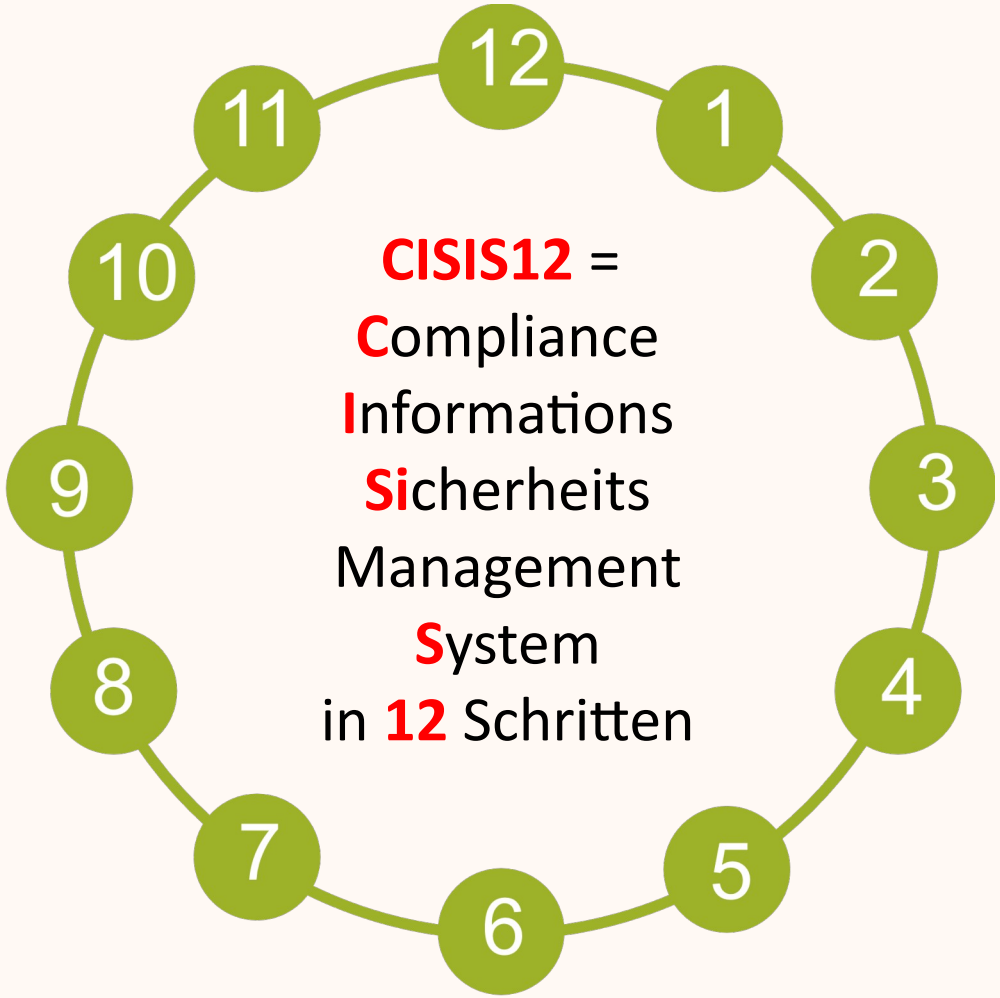
- *Energie*
  - Elektrizität -> Erzeuger, Verteiler, Übertragungsnetze, Ladepunkte.
  - Fernwärme/-kälte,
  - Öl (Produktion, Lager, Fernleitungen),
  - Gas (Versorgungs-, Verteilungs-, Fernleitungs-, Speichernetze),
  - Wasserstoff,
- *Verkehr* (Luft, Schiene, Schifffahrt, Straßenverkehr),
- *Gesundheit* (inkl. Dienstleister, Hersteller pharmazeutischer Produkte, Medizinprodukte, Referenzlabs der EU),
- *Finanzmarkt/Banken* (Kreditinstitute, Handelsplätze; Überschneidung DORA),
- (Trink-)Wasserversorger, Abwasser,
- *Digitale Infrastruktur* (Rechenzentren, Cloud/Computing, digitale Kommunikation, öffentliche Kommunikationsnetze),
- Verwaltung von IKT/B2B,
- Weltraum,
- Verwaltung, Regierung (nicht Justiz, Parlamente, Zentralbanken, Gefängnisse, Verteidigung),
- Post-/Kurierdienstleister,
- Abfallwirtschaft,
- Chemie (Produktion, Herstellung, Handel),
- Lebensmittel (Produktion, Verarbeitung, Handel),
- Verarbeitendes Gewerbe, Herstellung
- Medien, digitale Dienste (TV, Radio, Online-Shops, Suchmaschinen, Social-Media-Netze)
- Forschungseinrichtungen.

Was muss man tun?

- Governance (Artikel 20)
  - Verpflichtung zur Einhaltung von Risikomanagementmaßnahmen.
- Risikomanagement (Artikel 21)
- Berichtspflicht (Artikel 23)

CISIS12 ist…

- ein Informationssicherheitsmanagementsystem in zwölf Schritten,
- branchenunabhängig,
- leichtfüßig,
- besonders gut geeignet für kleine und mittständische Unternehmen (KMU),
- die Weiterentwicklung aus dem bereits gut etablierten Vorgänger ISIS12.
- Folgt dem PDCA-Zyklus,
- ist auditierbar, zertifizierbar *(nicht mit DAkkS-Zertifizierung verwechseln)*.



CISIS12-Schwerpunkte

- **Risikomanagement**,
- **Compliance/Governance** und zugehörige Prozesse (sämtlichst),
- strukturierten Aufbau: Norm, Maßnahmenkatalog, Auditschema,
- liefert Verweise zu relevanten Normen und Maßnahmen-Katalogen aus BSI-IT-Grundschutz und ISO/IEC 27001,
- bietet Integrationsmöglichkeiten von branchenspezifischen Normen und Katalogen, wie TISAX, B3S-KRITIS,
- wird ergänzt durch ein Handbuch, Schulungskonzept,
- umfasst einen Software-Markt mit unterschiedlichen Produkten, darunter Projektmanagement, DSGVO-Modul, Dokumentensteuerung,
- Zyklische (PDCA) Vorgehensweise.

Zwölf plus zwei Schritte in fünf Phasen

- 00: Startup
- **01: Leitlinie erstellen**
- **02: Beschäftigte sensibilisieren**
- 03: Informationssicherheitsteam aufbauen
- **04: IT-Dokumentation aufbauen**
- 05: IT-Servicemanagement
- 06: **Compliance**, Prozesse und Anwendungen
- 07: IT-Struktur analysieren
- **08: Risikomanagement**
- 09: Soll-Ist-Vergleich
- 10: Umsetzung planen und umsetzen
- 11: Internes Audit
- 12: Revision
- 13: Audit

Unterschiede Verordnung zu Richtlinie

- **Verordnung**: „Die V. dient der Schaffung des sog. sekundären Rechts (Art. 288 AEUV) und wird von Gemeinschaftsorganen erlassen. Die Europäische Kommission ist zumeist auf Durchführungsverordnungen beschränkt, welche aufgrund einer »Grundverordnung« erlassen werden. *Die Verordnung ist im Gegensatz zu Richtlinien in allen EU-Mitgliedstaaten mit »Durchgriffswirkung« für den Einzelnen unmittelbar gültig und rechtlich verbindlich*, ohne dass es einer Umsetzung (»Implementation«) in nationales Recht bedarf. Daher ist sie als Regelungstypus von ihren Rechtswirkungen her am ehesten mit einem gewöhnlichen innerstaatlichen Gesetz vergleichbar. Sie genießt im Kollisionsfall mit nationalem Recht allerdings Anwendungsvorrang.“ (M. Höreth, Das Europalexikon; Das Europalexikon | bpb.de)

- **Richtlinie**: „Die R. ist ein Rechtsakt, der der Schaffung des sog. sekundären Rechts dient (Art. 288 AEUV). Das Besondere an ihr ist, dass sie die Mitgliedstaaten der EU im Hinblick auf die innerhalb einer bestimmten Frist zu erreichenden Ziele bindet, ihnen aber – im Gegensatz zur Verordnung – bei der Umsetzung in nationales Recht die Wahl der Mittel überlässt, mit denen diese Ziele erreicht werden sollen. Auf diese Weise soll nicht nur die Entscheidungsfindung auf EU-Ebene erleichtert werden, sondern auch die Autonomie der nationalen Gesetzgeber trotz des europ. Regelungsbedarfs möglichst geschont werden.“(M. Höreth, Das Europalexikon; Das Europalexikon | bpb.de)

Vielen Dank für Ihre Aufmerksamkeit

IT-Sicherheitscluster e. V.

Dr. Matthias Kampmann

matthias.kampmann@it-sicherheitscluster.de

Franz-Mayer-Straße 1

D-93053 Regensburg

Tel.: +49 941 60488932