SPG SPECIFIC GROUP

WISTO

Webinar: NIS-2-Readiness – Regulierung verstehen, Umsetzung gestalten

Mag. Dzevad Mujezinovic, CIPP/E, CISM

05.05.2026

NIS2 Ready?

Risikomanagementmaßnahmen

Risikomanagementmaßnahmen im Bereich der Cybersicherheit

§ 32. (1) Wesentliche und wichtige Einrichtungen haben geeignete und verhältnismäßige Risikomanagementmaßnahmen in technischer, operativer und organisatorischer Hinsicht umzusetzen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu reduzieren und die Auswirkungen von Cybersicherheitsvorfällen auf die Nutzer ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

(2) Die Risikomanagementmaßnahmen haben zudem unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen nationalen, europäischen und internationalen Normen sowie bewährter Verfahren und der Kosten der Umsetzung ein Cybersicherheitsniveau zu gewährleisten, das dem bestehenden Risiko angemessen ist.

(3) Bei der Beurteilung der Verhältnismäßigkeit der Risikomanagementmaßnahmen sind das Ausmaß der Risikoexposition der Einrichtung sowie ihrer Dienste, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Cybersicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen.

(4) Diese Risikomanagementmaßnahmen haben auf einem gefahrenübergreifenden Ansatz zu beruhen, der auf den Schutz der Netz- und Informationssysteme samt deren physischen Komponenten vor Cybersicherheitsvorfällen abzielt, und zumindest folgende Inhalte zu umfassen:

a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;

b) Bewältigung von Cybersicherheitsvorfällen;

c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;

d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern, unter Berücksichtigung der spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Diensteanbieter, der Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Dienstanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse, sowie der Ergebnisse der gemäß Art. 22 Abs. 1 NIS-2-Richtlinie durchgeführten koordinierten Risikobewertungen;

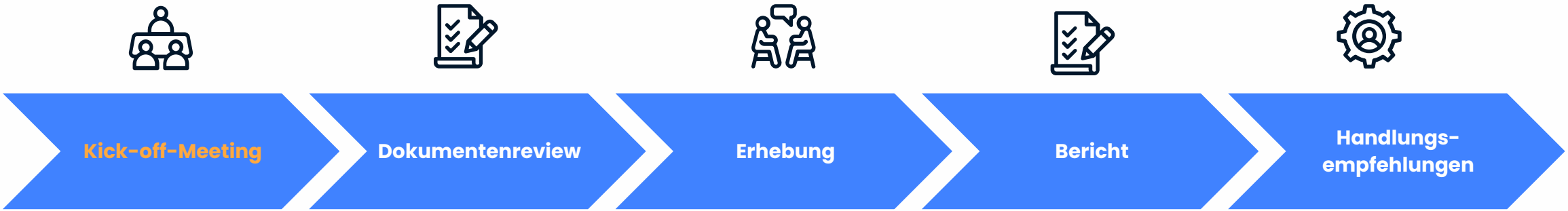
e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und

NIS2 Ready?

Effiziente NIS2-Gap-Analyse

NIS2 ist kein IT-Projekt sondern Management- und Governance-Thema!

Das Ziel einer Gap-Analyse für NIS2 ist es, die bestehenden Sicherheitsmaßnahmen eines Unternehmens mit den Anforderungen der NIS2-Richtlinie zu vergleichen bzw. NISG 2026, um Lücken und Handlungsbedarfe zur Compliance-Umsetzung zu identifizieren.



Zusammenarbeit

Governance!!!

Vorgehensweise

Herausforderungen IT/OT-Schnittstelle

- **Sicherheitslücken:** Fernwartung, IIoT, Cloud-Anbindungen

- Unterschiedliche Sicherheitslogiken in IT & OT

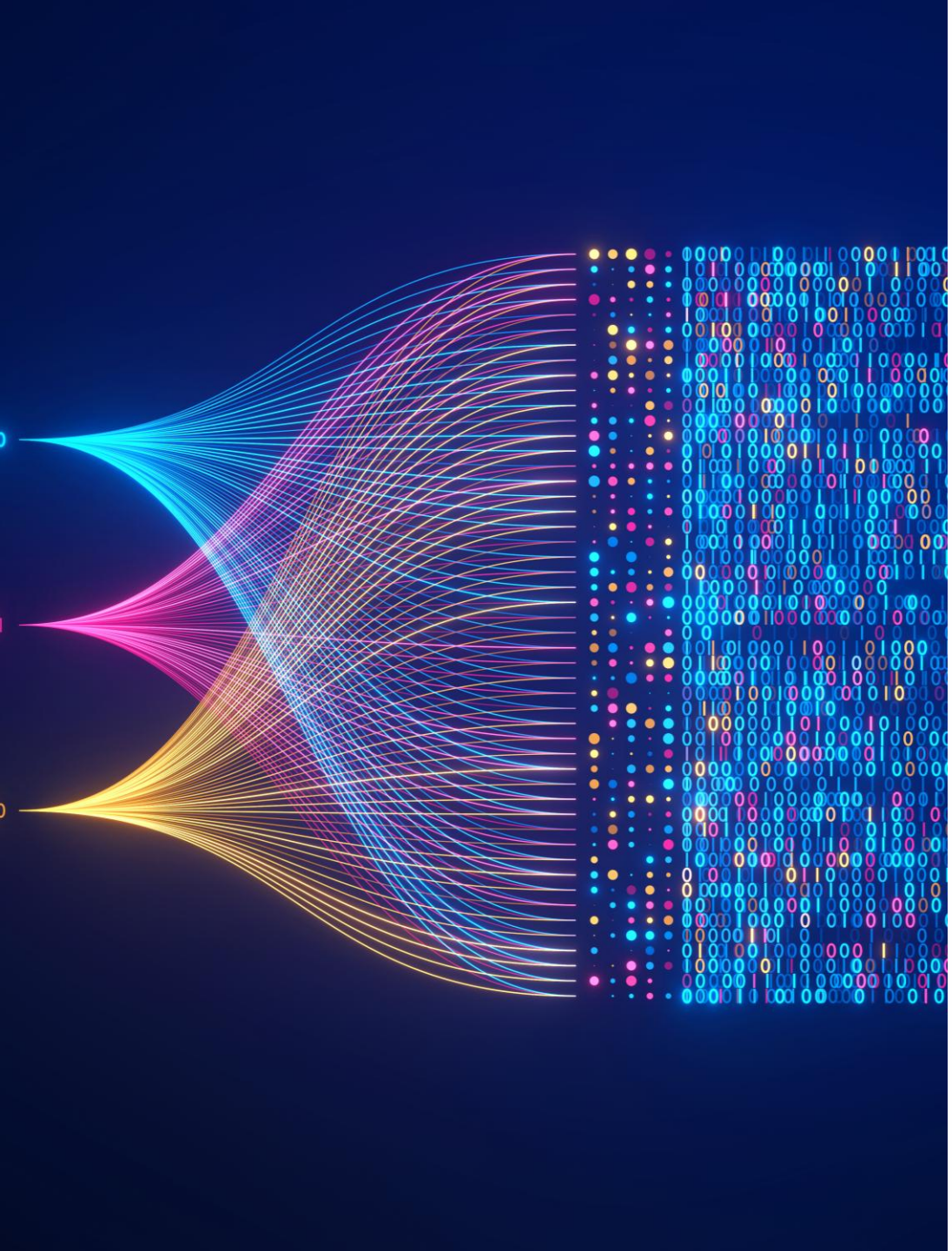
- NIS2 (ErwGr. 89, Art. 21): Netzwerksegmentierung, Zugriffskontrollen, Monitoring

- Praxis: IT & OT-Teams oft in Silos → **fehlende Zusammenarbeit**

NIS2 Ready?

Warum OT besonders betroffen ist?

- Angriffe auf OT haben reale Auswirkungen: Produktionsstillstände, Versorgungsausfälle, Sicherheitsrisiken
- OT = Steuerung und Überwachung physischer Prozesse (SCADA, DCS, PLCs, Robotik)
- Unterschiede zur IT: OT = Verfügbarkeit & Safety, IT = Vertraulichkeit & Integrität



Lieferkettensicherheit & IT-Outsourcing

- **Vertragliche Vorgaben:** Sicherheits- und Compliance-Anforderungen an alle Dienstleister
- **Risikobewertung:** Regelmäßige Prüfung von Lieferanten und IT-Partnern (Risikokriterien, Lieferanteninventar, Kritikalität bewerten, Maßnahmen ableiten). **Ersatz- oder Exit-Strategien** bei hohem Risiko!
- **Einbindung ins Incident Management:** Klare Melde- und Reaktionsprozesse mit Dritten
- **Kontinuierliches Monitoring:** Laufende Überwachung und Auditierung externer Leistungen

Standards und Frameworks für NIS2-Compliance

ISO 27001

- Internationaler Standard für ISMS
- 114 Controls in Annex A
- Zertifizierbar und auditierbar
- Risk-based Approach
- Dokumentationspflichten

NIST CSF 2.0

- 6 Kernfunktionen
- Flexibles Framework
- Maturity-Level Bewertung
- Supply Chain Integration
- Praktische Implementierung

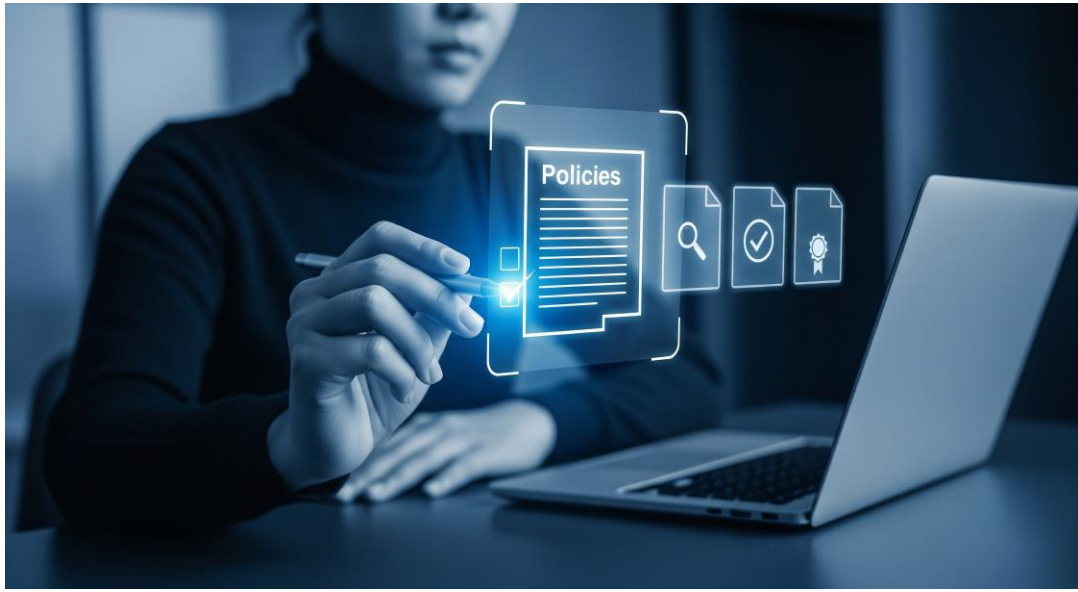
CIS Controls v8

- 18 priorisierte Controls
- Implementation Groups (IG1-IG3)
- Direkt umsetzbar
- Messbare Safeguards
- Community-getestet

BSI IT-Grundschutz-Standards ???

NIS2 Ready?

Warum Tools statt Excel?



- ✗ Manuelle Aktualisierung → **Automatische Workflows**
- ✗ Versionskonflikte → **Single Source of Truth**
- ✗ Keine Verknüpfungen → **Automatisches Relationship-Mapping**
- ✗ Fehleranfällig → **Validierung & Konsistenzprüfung**
- ✗ Keine Audit-Trails → **Vollständige Nachverfolgbarkeit**
- ✗ Keine Dashboards → **Echtzeit-Reporting & KPIs**
- ✗ Isolierte Silos → **Integrierte GRC-Sicht**

SPG

Vielen Dank! Haben Sie Fragen?

SPG SPECIFIC GROUP

Kontakt

Specific-Group Austria GmbH

Hoher Markt 5

1010 Wien

https://www.specific-group.com

Mag. Dzevad Mujezinovic, CIPP/E, CISM
Managing Director GRC Consulting
Head of GRC-Services

Dzevad.mujezinovic@specific-group.com

SPG ist Ihr pragmatischer und praxisorientierter Partner, der IT-Compliance und Information-Security einfach und effektiv macht. Wir kombinieren technische Expertise, langjährige, branchenübergreifende Erfahrung und operative Exzellenz.

Mission Statement