CERHA HEMPEL

RICHTLINIE (EU) 2022/2555

über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2-Richtlinie)

Radziv Hasanoski, Austria Power Grid AG

Boris Treml, CERHA HEMPEL Rechtsanwälte GmbH

Wien, Mai 2023

Zu den Personen

- **Radziv Hasanoski**, MSc (Information Security Manager der Austrian Power Grid AG - APG)
  - 8 Jahre Erfahrung in der IT-Prüfung und -Beratung mit Schwerpunkt Informationssicherheit
  - 3 Jahre bei der Austrian Power Grid als Information Security Manager
  - zertifizierter ISO 27001-Auditor und -Berater

- Ing. Mag. **Boris Treml**, LL.M. (CERHA HEMPEL Rechtsanwälte GmbH)
  - 10 Jahre Erfahrung in der IT
    - Programmierung, Projektmanagement
    - zertifizierter ISO 27001-Auditor
  - Umsetzung der NIS-Vorgaben im Sektor Verkehr und Energie
  - Beratungsschwerpunkt bei CERHA HEMPEL
    - Datenschutzrecht und IT-Informationssicherheitsrecht

Agenda

- **Einführung in die Informationssicherheit und die NIS-Regulierung**
- **Beschreibung einer konkreten technisch organisatorischen Umsetzung der NIS-Vorgaben (NISG und NISV) im Bereich der Energiewirtschaft**
- **Ausbildungs- und Haftungsaspekte**

Einführung in die Informationssicherheit

Metro kämpft weiter mit Cyberattacke

Lebensmittel Zeitung
https://www.lebensmittelzeitung.net › ...

IT-SICHERHEIT

Sicherheitslücke: Hacker kapern Jeep während Fahrt auf Autobahn

Eindringlinge konnten Bremsen manipulieren – Fiat Chrysler bittet Käufer, Update zu installieren

DER STANDARD

Prorussische Hacker greifen offenbar deutsche Flughäfen an

Nach einer entsprechenden Ankündigung prorussischer Hacker sind am Mittwoch die Webseiten zahlreicher Flughäfen ausgefallen. Auslöser für die Cyberangriffe ist die Entscheidung der Bundesregierung, die Ukraine mit ützen.

NETZPOLITIK

Grundversorgung weg, Politikerdaten im Netz: Wie Hacker Kärnten lahmlegten

Der Cyberangriff auf Kärnten ist exemplarisch dafür, wie Hacker seit Beginn der Pandemie vorgehen

Muzayen Al-Youssef, Walter Müller
13. Juni 2022, 06:00, 479 Postings

CYBER-SECURITY

Palfinger zahlte Lösegeld, um globalen Cyberangriff abzuwehren

Ende Jänner gelang es Hackern, für rund zwei Wochen einen Großteil der weltweiten Standorte des Kranbauunternehmens lahmzulegen

23. März 2021, 11:55, 264 Postings

anuar 2023, 17:05 Uhr

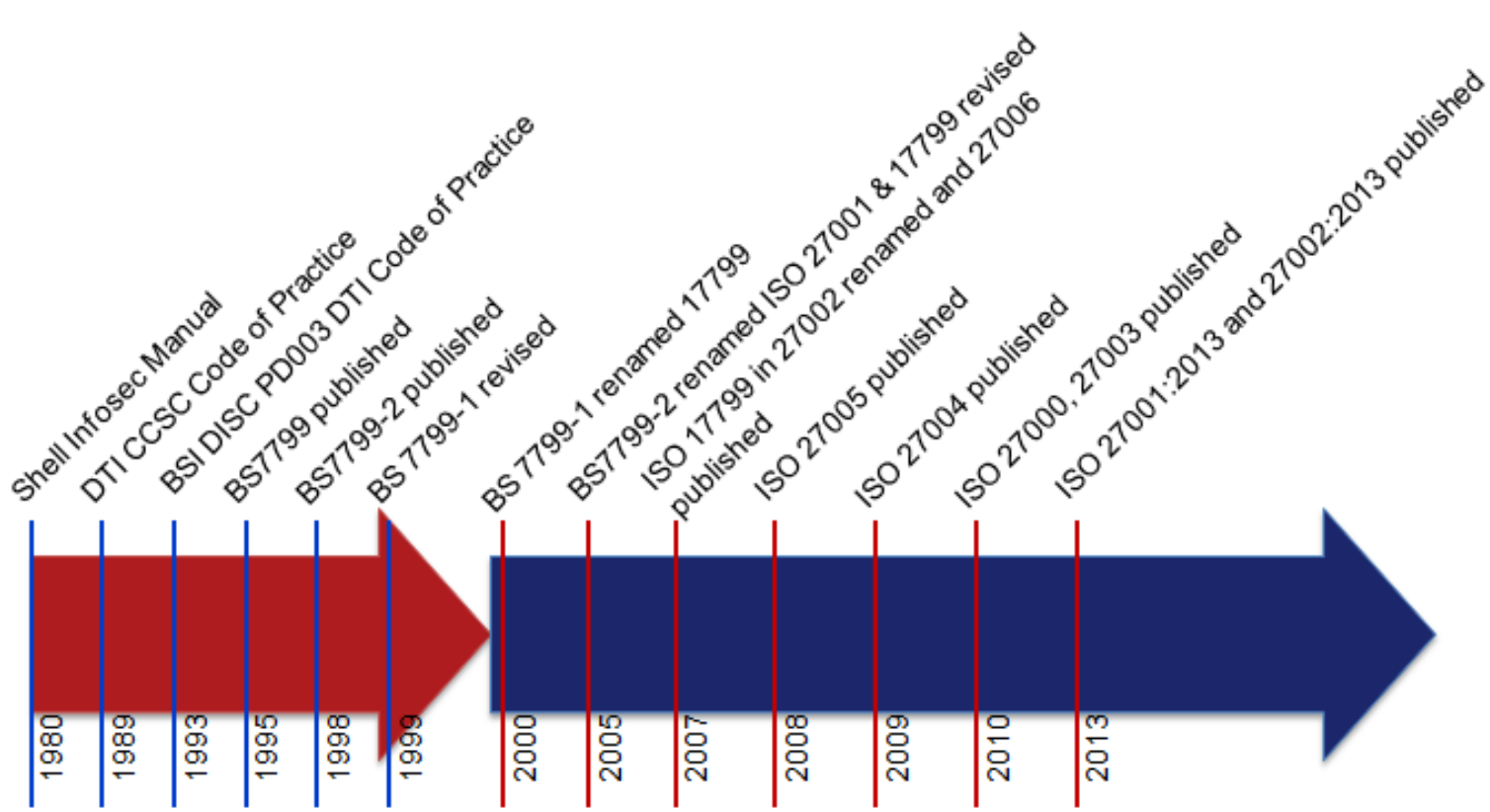
Einführung in die Informationssicherheit

Begriffsdefinition

- „Netz- und Informationssystemsicherheit (NIS)“ bedeutet die Fähigkeit, Sicherheitsvorfällen vorzubeugen, diese zu erkennen, abzuwehren und zu beseitigen (§ 3 Z 2 NISG)

- „Sicherheit von Netz- und Informationssystemen“ bedeutet die Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten Vertrauensniveau alle Ereignisse abzuwehren, die die **Verfügbarkeit**, **Authentizität**, **Integrität** oder **Vertraulichkeit** gespeicherter oder übermittelter oder verarbeiteter Daten oder der Dienste, die über diese Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen können (Art 6 Z 2 NIS2-RL)

Einführung in die Informationssicherheit



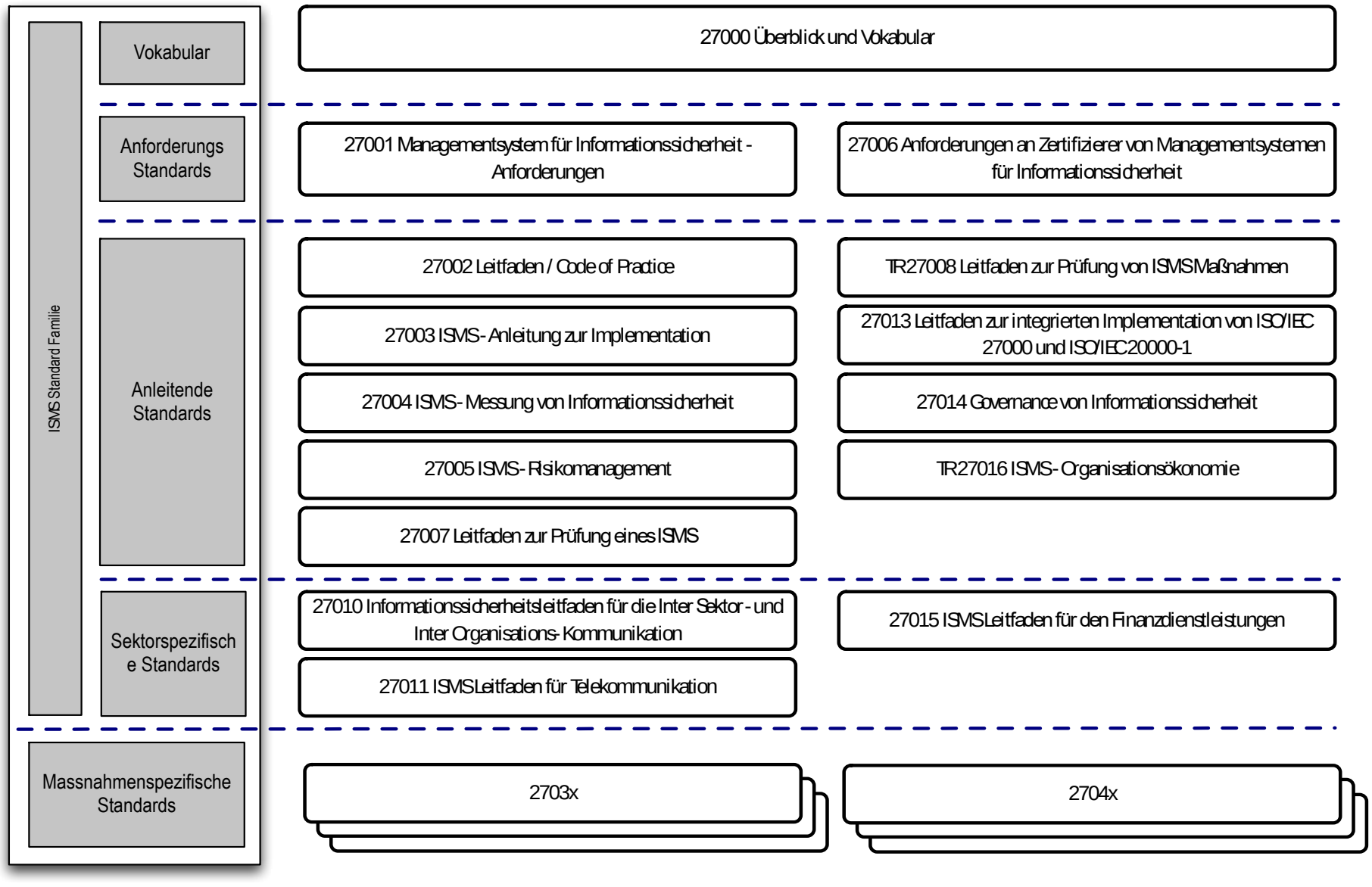
Einführung in die Informationssicherheit

Zwei Denkschulen

- **ISO/IEC 27001:2013**
  - industrieller Standard
  - abstrakte Norm mit Empfehlungen, aber ohne konkrete Umsetzungsvorgaben
  - Umfang: 31 Seiten
- **IT-Grundschutz**
  - Bundesamt für Sicherheit in der Informationstechnik (Deutschland), 1.430 Mitarbeiter
  - umfangreiche Sammlung von Katalogen mit konkreten Maßnahmen
  - Gesamtumfang: ca. 4.800 Seiten
  - BSI-Standards
    - BSI-Standard 100-1: Managementsysteme für Informationssicherheit
    - BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
    - BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
- **Österreichisches Informationssicherheitshandbuch**
  - Bundeskanzleramt
  - Sammlung konkreter Vorgaben zur Informationssicherheit
  - Umfang: 708 Seiten

Einführung in die Informationssicherheit

Die ISO 270xx Familie



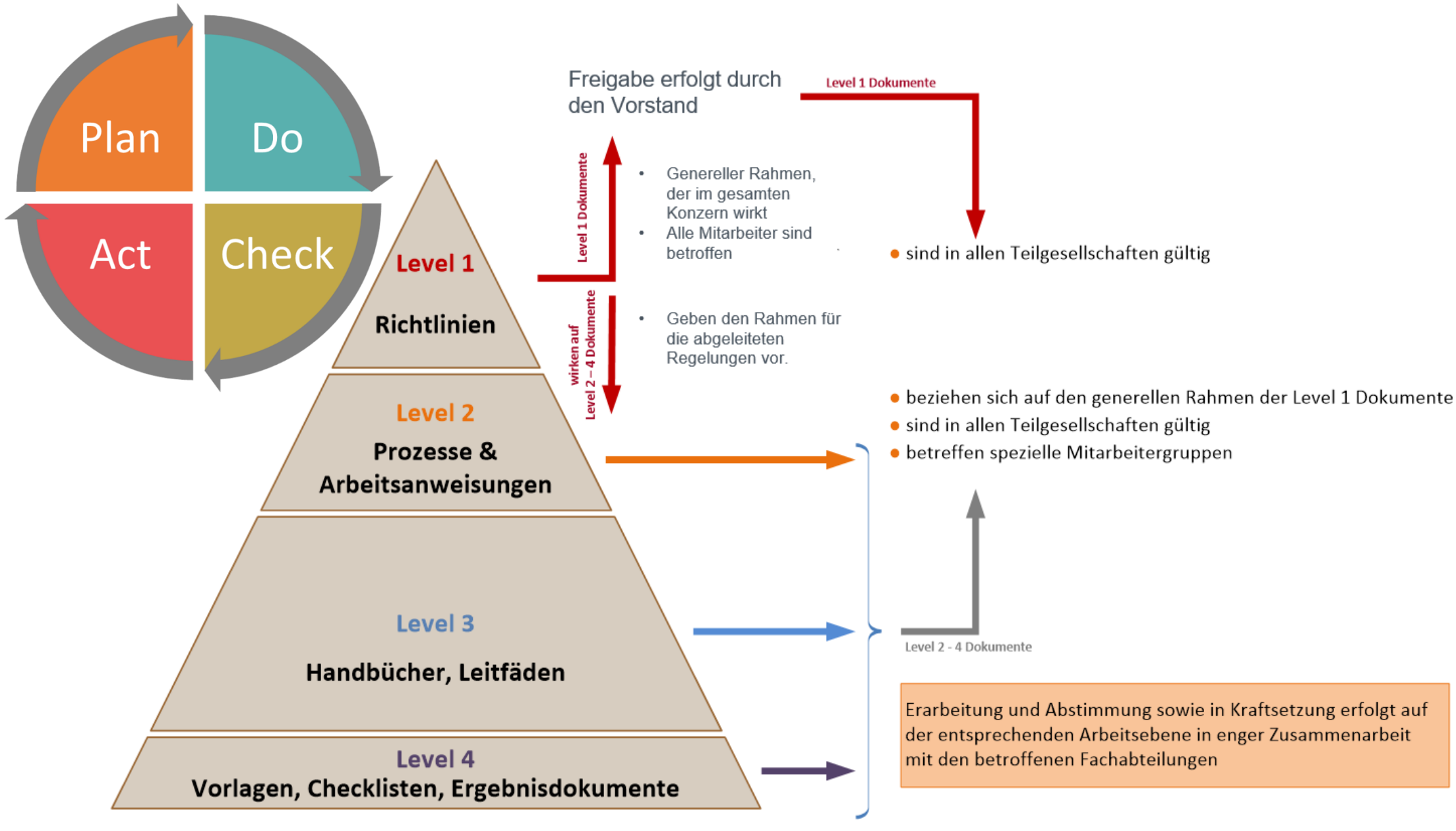
Einführung in die Informationssicherheit

Information Security Management System

- Ein Information Security Management System (ISMS) ist eine Festlegung von Verfahren und Regeln innerhalb eines Unternehmens, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Dabei werden technische und nichttechnische Aspekte berücksichtigt.

Einführung in die Informationssicherheit

Umsetzung eines ISMS



Einführung in die Informationssicherheit

Struktur der ISO/IEC 27001:2013

0. Einleitung (Introduction)
1. Anwendungsbereich (Scope)
2. Normative Verweise (Normative references)
3. Begriffe (Terms and Definitions)
4. Umfeld der Organisation (Context of the organization)
5. Führung / Leitung (Leadership)
6. Planung (Planning)
7. Unterstützung (Support)
8. Betrieb (Operation)
9. Leistungskontrolle (Performance evaluation)
10. Verbesserung (Improvement)

Anhang A (Normativ) - Maßnahmenziele und Maßnahmen (Annex A (normative) - Reference control objectives and controls)

Normativ

Abschnitte des ISO/IEC 27001 Annex A

- 5 – Informationssicherheitsrichtlinien
- 6 - Organisation der Informationssicherheit
- 7 - Personalsicherheit
- 8 - Verwaltung der Werte
- 9 - Zugangssteuerung
- 10 - Kryptographie
- 11 - Physische und umgebungsbezogene Sicherheit
- 12 - Betriebssicherheit
- 13 - Kommunikationssicherheit
- 14 - Anschaffung, Entwicklung und Instandhaltung von Systemen
- 15 - Lieferantenbeziehungen
- 16 - Handhabung von Informationssicherheitsvorfällen
- 17 - Informationssicherheitsaspekte beim Business Continuity Management
- 18 - Compliance

ZERTIFIKAT ■ CERTIFICADO ■ CERTIFICAT ■ СЕРТИФИКАТ ■ 認證證書

Management Service

ZERTIFIKAT

Die Zertifizierun
der TÜV SÜD Manageme
bescheinigt, dass das

DATAGR
IT Services + S

DATAGROU
Bereich IT Se
Wilhelm-Schickar
72124 Pliezh
Deutschla

einschließlich der Standc

ein Managementsystem
eingeführt hat und

Das Service Manage
das die Erbringung aller
enthaltenen Services für alle
IT Services der DATAGRO

Durch ein Audit, Bericht
wurde der Nachweis erbracht, d

ISO/IEC 2000

erfüllt sin

Dieses Zertifikat ist gültig vom 20
Zertifikat-Registrier-Nr.: 12

M. Weg

Product Compliance M
München, 2015-

Seite 1 von

TÜV SÜD Management Service GmbH • Zertifizierungsstelle • Ridler
www.tuev-sued.de/certificate-valic

DATAGROUP AG
Bereich IT Services
Wilhelm-Schickard-Straße 7
72124 Pliezhausen
Deutschland

einschließlich der Standorte gemäß Anlage

ein Managementsystem für IT-Services
eingeführt hat und anwendet.

Das Service Management System,
das die Erbringung aller im Servicekatalog
enthaltenen Services für alle Kunden des Bereiches
IT Services der DATAGROUP AG unterstützt.

Durch ein Audit, Bericht-Nr. **70793815**,
wurde der Nachweis erbracht, dass die Forderungen der

ISO/IEC 20000-1:2011

erfüllt sind.

Beschreibung einer konkreten technisch organisatorischen Umsetzung der NIS-Vorgaben (NISG und NISV) im Bereich der Energiewirtschaft

NIS1 - Kinderkrankheiten

Beweggründe für die Neufassung

Unzureichendes Niveau der Cyber-Resilienz von Unternehmen aufgrund von

- fehlenden Cybersicherheitsmaßnahmen (aufgrund der Nichtberücksichtigung)
- uneinheitlicher Behandlung im gesamten Binnenmarkt (Diskrepanzen bei den Ermittlungen der Betreiber wesentlicher Dienste)
- unterschiedlich starker Resilienz der Mitgliedstaaten und Sektoren
- schwach ausgeprägter gemeinsamer Lageerfassung und mangelnder gemeinsamer Krisenreaktion

Fleckerlteppich der IT-Sicherheits-Regulierung

Cyber Resilience Act*

- Cyber Resilience Act – gilt für die Entwicklung und Markteinführung von digitalen Produkten
- (i) Verantwortlichkeit der Hersteller während des Lebenszyklus der digitalen Produkte
- (ii) mehr Transparenz über die Sicherheit von Hard- und Softwareprodukten und
- (iii) Meldepflichten, Risikobewertung, Schwachstellenanalyse für 5 Jahre ab Produkteinführung

Cybersecurity Act

- Ziele und Aufgaben der ENISA (Agentur der Europäischen Union für Cybersicherheit)
- Cybersicherheitszertifizierung zur Herstellung einer adäquaten Cybersicherheit

NIS2-Regulierung

Pflichten an die Mitgliedstaaten

Wesentliche und wichtige Einrichtungen

Digital Operational Resilience Act (DORA)

* Vorhaben

NIS2

Adressatenkreis (Art 3 NIS2-RL)

Wesentliche Einrichtungen (insbesondere):	**Wichtige Einrichtungen:**
•Energie •Verkehr •Bankwesen •Finanzmarktinfrastrukturen •Gesundheitswesen •Trinkwasser •Abwasser •digitale Infrastruktur •Verwaltung von IKT-Diensten B2B •öffentliche Verwaltung •Weltraum •qual. Vertrauensdienstanbieter •Domänennamenregister der Domäne oberster Stufe sowie DNS-Diensteanbieter •Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienst •**Einrichtungen öffentlicher Verwaltung**	•Post- und Kurierdienste •Abfallbewirtschaftung •Chemie •Lebensmittel •verarbeitendes/herstellendes Gewerbe •Anbieter digitaler Dienste •Forschung (fakultativ)

- Adressatenkreis idR: mindestens mittlere Unternehmen (250 Mitarbeiter, 50 Mio Euro) (Art 2 NIS2-RL)

NIS2

Anforderungen

- **Cybersecurity als Compliance-Thema**
- **Leitungsorgane**
  - haben die Risikomanagementmaßnahmen zu genehmigen,
  - haben deren Umsetzung zu überwachen und
  - können für Verstöße verantwortlich gemacht werden (Art 20 Abs 1 NIS2-RL).
- **Aufsicht durch Behörden**
  - Vor-Ort-Kontrollen,
  - Ad-hoc-Prüfungen durch **Sicherheitsaudits** und Sicherheitsscans (Art 32 f NIS2-RL)
  - **Wesentliche Einrichtungen** unterliegen einer umfassenden Ex-ante- und Ex-post-Aufsicht (ErwGr 122)
  - Pflicht zur systematischen Dokumentation des Risikomanagementsystems
  - **Bei Verstößen drohen Bußgelder von 10 Mio. EUR oder 2 % des weltweiten Jahresumsatzes (Art 34 Abs 4 NIS2-RL)**

Verantwortung der Leitungsorgane

Unmittelbare Genehmigung der Maßnahmen und unmittelbare Haftung der Leitungsorgane

- Art 20 Abs 1 NIS2-RL: Die Mitgliedstaaten stellen sicher, dass die Leitungsorgane wesentlicher und wichtiger Einrichtungen die von diesen Einrichtungen zur Einhaltung von Artikel 21 ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit **billigen**, **ihre Umsetzung überwachen** und für Verstöße gegen diesen Artikel durch die betreffenden **Einrichtungen verantwortlich** gemacht werden können.

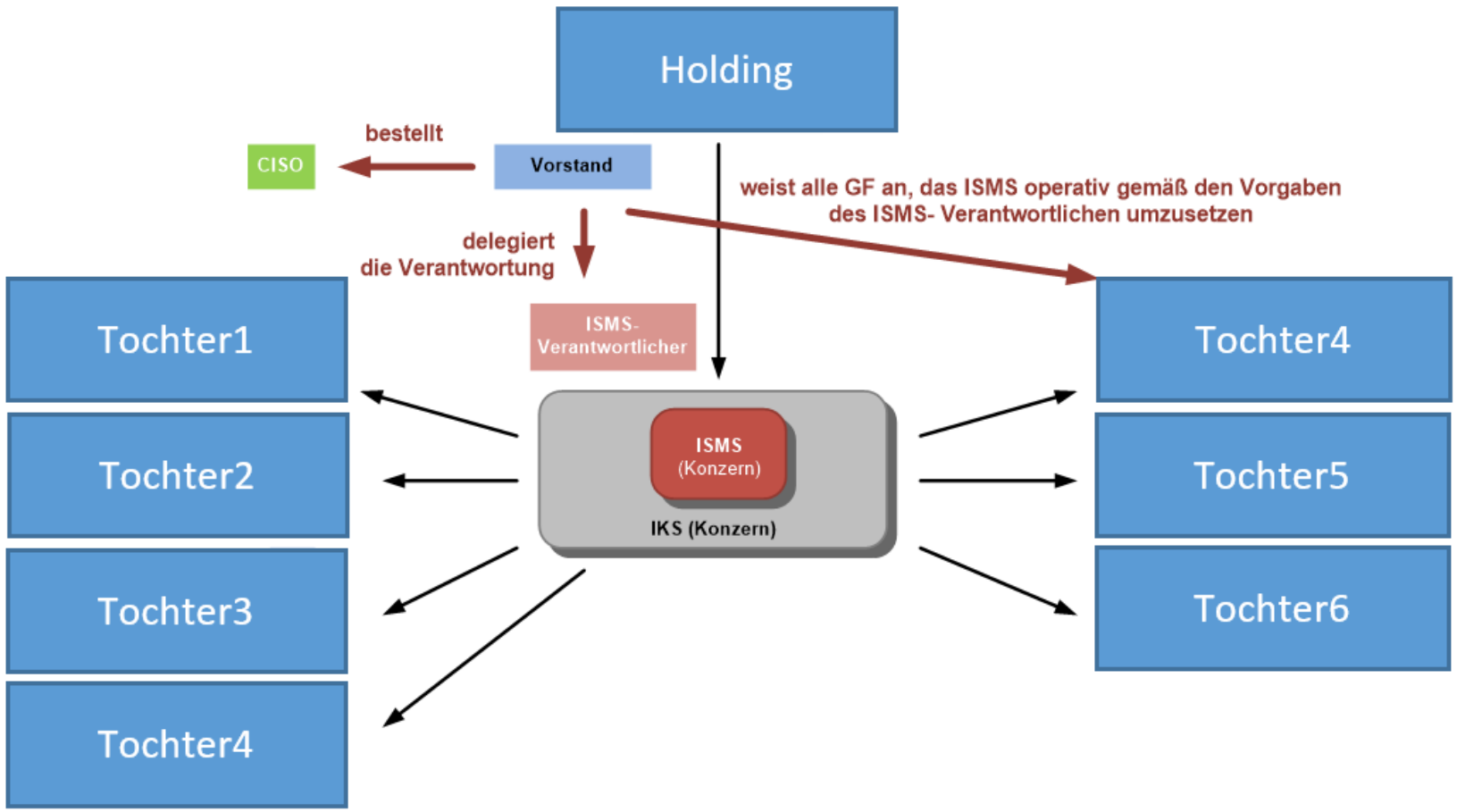
Schulungen für Leitungsorgane

- Art 20 Abs 2 NIS2-RL: Die Mitgliedstaaten stellen sicher, dass die Mitglieder der **Leitungsorgane** wesentlicher und wichtiger Einrichtungen an **Schulungen teilnehmen müssen**, und fordern wesentliche und wichtige Einrichtungen auf, **allen Mitarbeitern regelmäßig** entsprechende Schulungen anzubieten, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

Organisatorischer Aufbau

Möglichkeiten zur Umsetzung

zentrale Umsetzung



CISO

weisungsfrei für
- Design
- Implementierung
- Prüfung der operativen Wirksamkeit

aller ISMS-Belange

ISMS-Verantwortlicher

weisungsbefugt für
- Design
- prozesstechnische Implementierung des ISMS in den Gesellschaften
- Prüfung der operativen Wirksamkeit

aller ISMS-Belange

Leitungsorgan

weisungsbefugt für
- Design
- technische Implementierung von IT-Lösungen gemäß den ISMS-Vorgaben
- Prüfung der operativen Wirksamkeit

aller ISMS-Belange

Anpassung der IT-Sicherheit

- **NIS1-RL: Nur jene Services sind betroffen, die für den Betrieb des wesentlichen Dienstes notwendig sind. (ErwGr 22 NIS1-RL).**
- Art 21 NIS2-RL: Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten
- **All-hazards approach:** ist ein umfassender Ansatz für die Vorbereitung auf Notfälle, der das gesamte Ausmaß von Notfällen oder Katastrophen bei der Planung von Reaktionskapazitäten und Maßnahmen zur Schadensbegrenzung berücksichtigt. Dies bedeutet, dass Sie auf "alle Gefahren" vorbereitet sind, denen Ihr Unternehmen ausgesetzt sein könnte.
  - Intern
  - Extern
  - Naturkatastrophen

Anforderungen an die IT-Sicherheit (Art 21 NIS-RL)

- Risikoanalyse und Sicherheitsrichtlinien für Informationssysteme
- **Sicherheit** bei der **Beschaffung**, **Entwicklung** und **Wartung** von **Netz- und Informationssystemen**
- Behandlung von Vorfällen
- Business Continuity (inkl. Backup-Management und Notfallwiederherstellung) und Krisenmanagement
- Supply Chain Security (inkl. sicherheitsbezogene Aspekte der Beziehungen mit direkten Anbietern oder Diensteanbietern)
- einschließlich Umgang mit Schwachstellen und deren Offenlegung
- Richtlinien und Verfahren zur Bewertung der Wirksamkeit von Cyber-Risikomanagementmaßnahmen
- grundlegende Praktiken der Cyberhygiene und Schulungen zur Cybersicherheit
- Richtlinien und Verfahren zum Einsatz von Kryptografie und, wo angemessen, Verschlüsselung
- Sicherheit der Humanressourcen, Zugangskontrollmaßnahmen und Vermögensverwaltung
- Verwendung von Lösungen für die MFA oder die kontinuierliche Authentifizierung, die gesicherte Sprach-, Video- und Textkommunikation sowie ggf gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung

Aufsichtsmaßnahmen und Strafen

- **Aktuell 50.000 Euro, im Wiederholungsfall 100.000 Euro.**

- Strafhöhe wird auf mindestens 10 Mio Euro oder bis zu 2 % des weltweiten Gesamtjahresumsatz für wesentliche Einrichtungen “gehoben” (Art 34 Abs 4 NIS2-RL).
- Leitungsorgane können für Pflichtverletzungen haftbar gemacht werden
  (siehe etwa Art 20 Abs 1 NIS2-RL).

CERHA HEMPEL

Vielen Dank für Ihre Aufmerksamkeit