Cybersicherheit ist Chefsache

Gezielte Vorbereitung auf NIS-2!

Dr. Heidrun Benda

Kurzvorstellung LSI

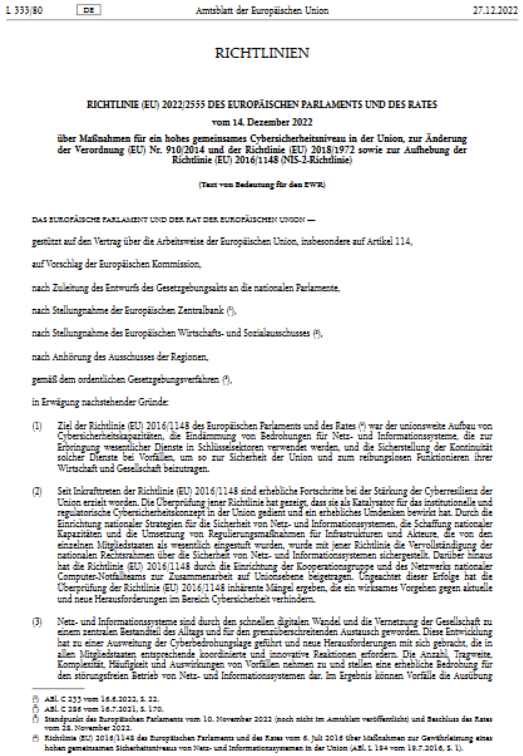
- Bayern als erstes Bundesland mit eigenem Landesamt
- LSI ist dem StMFH nachgeordnet
- Gründungszeitpunkt 01.12.2017
- Standorte:
  - Nürnberg
  - AS Würzburg
  - AS Bad Neustadt a. d. Saale
- Gesetzesgrundlage: BayDiG

NIS-2 und deutsche Umsetzung

NIS-2

- Richtlinie (EU) 2022/2555 des europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union
- Keine „unmittelbare“ Geltung
- Umwandlung in nationales Recht durch Mitgliedstaaten erforderlich

Ziel: Cybersicherheitsniveau harmonisieren und verbessern



L 333/80 DE Amtsblatt der Europäischen Union 27.12.2022

RICHTLINIEN

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 14. Dezember 2022

über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 114,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme der Europäischen Zentralbank (1),

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses (2),

nach Anhörung des Ausschusses der Regionen,

gemäß dem ordentlichen Gesetzgebungsverfahren (3),

in Erwägung nachstehender Gründe:

(1) Ziel der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates (4) war der unionsweite Aufbau von Cybersicherheitskapazitäten, die Eindämmung von Bedrohungen für Netz- und Informationssysteme, die zur Erbringung wesentlicher Dienste in Schlüsselsektoren verwendet werden, und die Sicherstellung der Kontinuität solcher Dienste bei Vorfällen, um so zur Sicherheit der Union und zum reibungslosen Funktionieren ihrer Wirtschaft und Gesellschaft beizutragen.

(2) Seit Inkrafttreten der Richtlinie (EU) 2016/1148 sind erhebliche Fortschritte bei der Stärkung der Cyberresilienz der Union erzielt worden. Die Überprüfung jener Richtlinie hat gezeigt, dass sie als Katalysator für das institutionelle und regulatorische Cybersicherheitskonzept in der Union gedient und ein erhebliches Umdenken bewirkt hat. Durch die Einrichtung nationaler Strategien für die Sicherheit von Netz- und Informationssystemen, die Schaffung nationaler Kapazitäten und die Umsetzung von Regulierungsmaßnahmen für Infrastrukturen und Akteure, die von den einzelnen Mitgliedstaaten als wesentlich eingestuft wurden, wurde mit jener Richtlinie die Vervollständigung der nationalen Rechtsrahmen über die Sicherheit von Netz- und Informationssystemen sichergestellt. Darüber hinaus hat die Richtlinie (EU) 2016/1148 durch die Einrichtung der Kooperationsgruppe und des Netzwerks nationaler Computer-Notfallteams zur Zusammenarbeit auf Unionsebene beigetragen. Ungeachtet dieser Erfolge hat die Überprüfung der Richtlinie (EU) 2016/1148 inhärente Mängel ergeben, die ein wirksames Vorgehen gegen aktuelle und neue Herausforderungen im Bereich Cybersicherheit verhindern.

(3) Netz- und Informationssysteme sind durch den schnellen digitalen Wandel und die Vernetzung der Gesellschaft zu einem zentralen Bestandteil des Alltags und für den grenzüberschreitenden Austausch geworden. Diese Entwicklung hat zu einer Ausweitung der Cyberbedrohungslage geführt und neue Herausforderungen mit sich gebracht, die in allen Mitgliedstaaten entsprechende koordinierte und innovative Reaktionen erfordern. Die Anzahl, Tragweite, Komplexität, Häufigkeit und Auswirkungen von Vorfällen nehmen zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von Netz- und Informationssystemen dar. Im Ergebnis können Vorfälle die Ausübung

(1) ABl. C 233 vom 16.6.2022, S. 22.
(2) ABl. C 286 vom 16.7.2021, S. 170.
(3) Standpunkt des Europäischen Parlaments vom 10. November 2022 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 28. November 2022.
(4) Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

NIS-2: Umsetzung in nationales Recht

- Frist für Umsetzung: 17. Oktober 2024
- Umsetzung durch das „NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz“ (NIS2UmsuCG)
  - Zeitraum für Umsetzung aktuell **unklar**

ZDNet / Cybersicherheit

NIS2: EU leitet Verfahren gegen Deutschland ein

Es geht auch um die Umsetzung der Richtlinie über die Resilienz kritischer Einrichtungen. Auch mehr als 20 weitere Mitgliedsstaaten haben beide Regulierungswerke noch nicht vollständig umgesetzt.

von **Stefan Beiersmann** am **2. Dezember 2024** , 09:15 Uhr

Hohe Schäden durch Cybercrime!

265 Milliarden Euro **Schaden**

Social Engineering
bei fast jedem zweiten Unternehmen

Top-3-Angriffe
- **Schadsoftware**
- **Phishing**
- Angriffe auf **Passwörter**

ca. 80 % der Unternehmen von Angriffen betroffen

Quelle: bitkom „Wirtschaftsschutz 2024“

LSI: Beratungsunterlagen für KMUs!

- Obwohl nationale Umsetzung der Richtlinie noch ausstehend ist: Vorbereitung und Umsetzung sinnvoll und dringend notwendig!
- Angebot des LSI:
  - Checkliste nach NIS-2-Kriterien
  - Handlungsempfehlung und Vorgehensmodell für KMUs

Vorstellung NIS-2-Checkliste

Betroffenheit prüfen

- Sektorenzugehörigkeit
- Kennzahlen (Angestellte, Jahresbilanz, Umsatz)

Betroffenheit prüfen: Regulierte Sektoren*

Anlage I	Anlage II
1. Energie	1. Post- und Kurierdienste
2. Transport und Verkehr	2. Abfallbewirtschaftung
3. Finanzwesen	3. Produktion, Herstellung und Handel mit chemischen Stoffen
4. Gesundheit	4. Produktion, Verarbeitung und Vertrieb von Lebensmitteln
5. Wasser	5. Verarbeitendes Gewerbe/Herstellung von Waren
6. Digitale Infrastruktur	6. Anbieter digitaler Dienste
7. Weltraum	7. Forschung

*nach NIS2UmsuCG (Stand 2.10.2024)

Betroffenheit prüfen: Einrichtungsarten

Wichtige Einrichtung (wE)	Besonders wichtige Einrichtung (bwE)	Betreiber kritischer Anlagen
Zugehörigkeit zu Anlage 1 oder 2	Zugehörigkeit zu Anlage 1	Sektoren nach § 4 (1) KRITIS-Dachgesetz und Verordnung
➢ Ab 50 Mitarbeiter ODER ➢ Ab 10 Mio. € Jahresumsatz und Jahresbilanzsumme	➢ Ab 250 Mitarbeiter ODER ➢ Ab 50 Mio. € Jahresumsatz und 43 Mio. € Jahresbilanzsumme	Mit Überschreitung der Schwellenwerte der Verordnung (Wassergewinnung beispielsweise derzeit ab 22 Mio. m³/Jahr)

Registrierungspflicht

- Betroffenheitsfeststellung: Pflicht der Unternehmen
- Wo?
  - Gemeinsame Meldestelle von BSI und BBK
- Wann?
  - Spätestens 3 Monate nachdem sie (besonders) wichtige Einrichtung sind
- Verstoß gegen Registrierung ist Ordnungswidrigkeit
  - Bußgeld in Höhe von 500.000 € möglich

Einige Risikomanagementmaßnahmen (§ 30)

- Risikoanalyse
- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung des Betriebs
- Sicherheit der Lieferkette
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen
- Cyberhygiene und Schulungen
- Kryptokonzept
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle
- Multi-Faktor-Authentifizierung, gesicherte Kommunikation und Notfallkommunikation innerhalb der Einrichtung

Dokumentation!

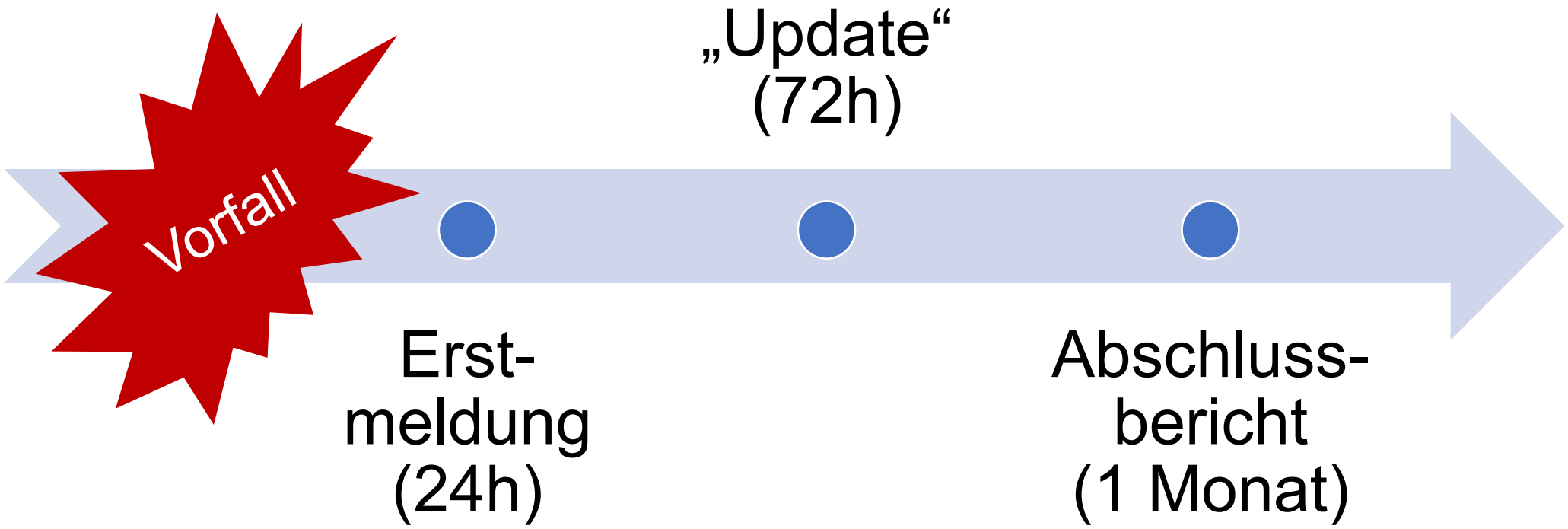
Pflichten der Geschäftsleitung

- Umsetzung und Überwachung der Risikomanagementmaßnahmen
- Pflicht zu Schulung
- Haftung bei Pflichtverletzung

Nachweispflicht

	Wichtige Einrichtung	Besonders wichtige Einrichtung	Kritische Anlage
Pflicht	§ 62	§ 61	§ 39 (1)
Form	„Prüfungen“	„Prüfungen“	Audits
Inhalt	Nachweis der umgesetzten Maßnahmen	Nachweis der umgesetzten Maßnahmen	Nachweis der umgesetzten Maßnahmen; SzA
Frequenz	Bei Anlass	Stichproben	Alle drei Jahre
Empfänger	BSI	BSI	BSI
	Regelungsintensität		

Meldepflichten bei Vorfällen



Sanktionen

Bei wichtigen Einrichtungen bis zu

- 7 Millionen € oder
- 1,4 % des Jahresumsatzes falls dieser > 500 Mio. €

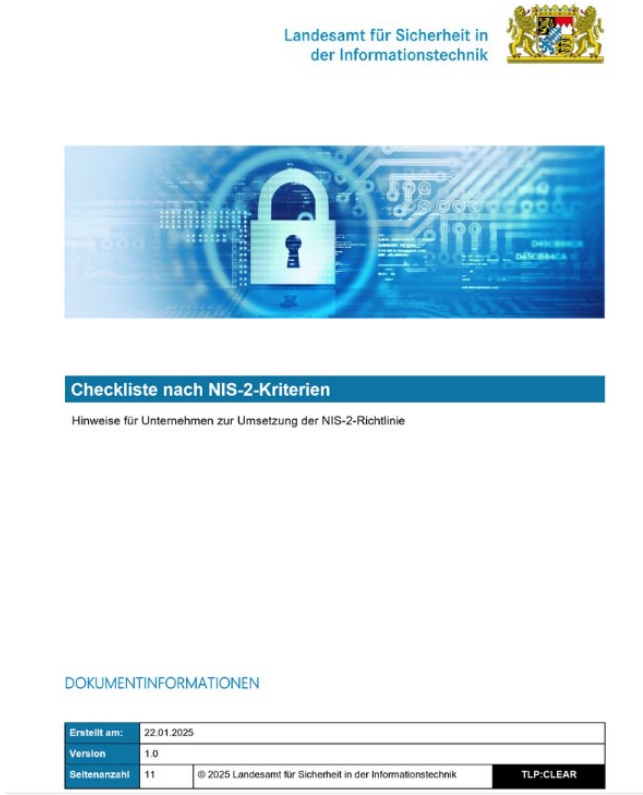
Bei besonders wichtigen Einrichtungen bis zu

- 10 Millionen € oder
- 2 % des Jahresumsatzes falls dieser > 500 Mio. €

„Checkliste nach NIS-2 Kriterien“

- NIS-2 FAQ
- NIS-2 Checkliste
- Sanktionen
- Weitere Empfehlungen und Hilfestellungen
- Weiterführende Hinweise
- Glossar

https://lsi.bayern.de/aktuelles/downloads/index.php



„Informationssicherheit für kleine und mittlere Unternehmen“

- Orientierungshilfe = Handlungsempfehlung (Excel) + Vorgehensmodell (PDF)
- Zielgruppe: Kleine und mittlere Unternehmen
- Grad der Informationssicherheit: Bereits gute Absicherung, unter dem geforderten Niveau für ein Nachweisverfahren (Sicherheitsaudit, Zertifizierung)
- Struktur: 12 Cluster, 89 Maßnahmen und insgesamt 266 Fragen
- Download: https://lsi.bayern.de/aktuelles/downloads/index.php

Vorgehensmodell

Vorschlag für eine zeitliche Reihenfolge

Stufe 0

Voraussetzung für den Start

Stufe 1

Bestandsaufnahme

Stufe 2

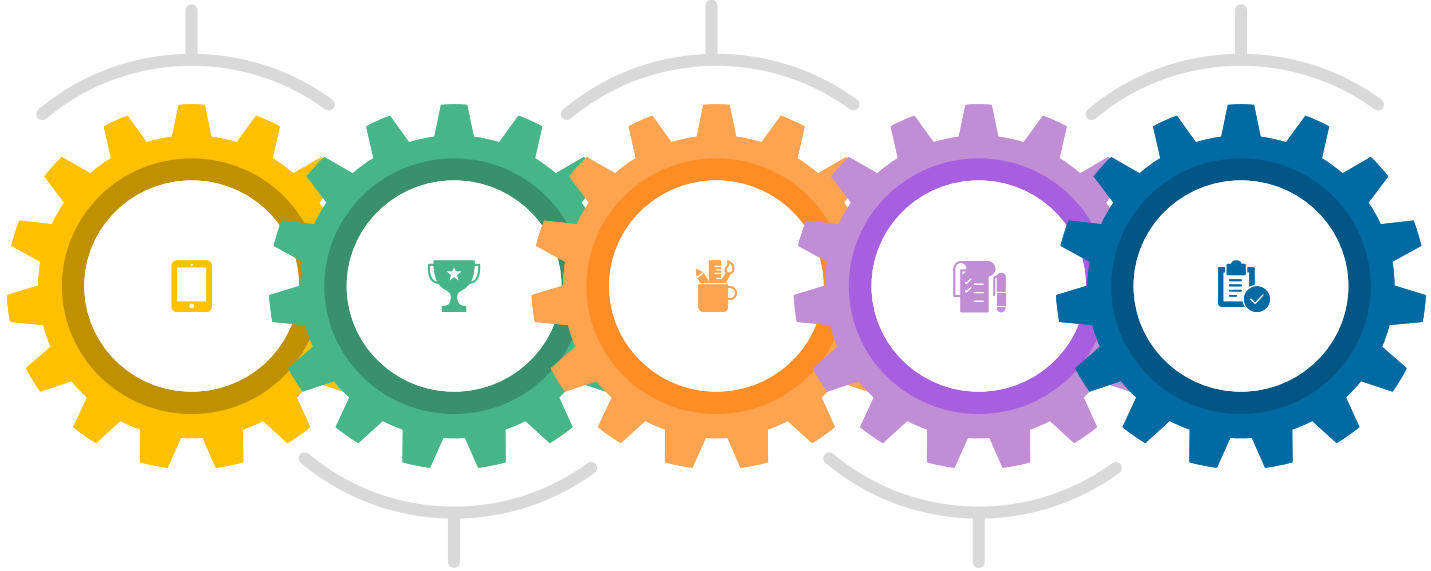
Organisatorische Maßnahmen und erste dringliche Absicherungen

Stufe 3

Weitere wichtige Absicherungen, Richtlinien und Dokumentation

Stufe 4

Aufrechterhaltung der Informationssicherheit und kontinuierliche Weiterentwicklung



Fallbeispiele

Betroffenheitsprüfung: Schmankerl Paradies GmbH

- Firma produziert bayerische Feinkost auf höchstem kulinarischen Niveau
- 40 Angestellte
- Jahresumsatz 7 Mio. €
- Jahresbilanzsumme 5 Mio. €

Sektor prüfen

Nr.	Sektor	Branche	Einrichtungsart
4.1.1	Produktion, Verarbeitung und Vertrieb von Lebensmitteln		Lebensmittelunternehmen nach Artikel 3 Nummer 2 der Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates vom 28. Januar 2002 […]

Prüfung der Size-cap-Regel

Wichtige Einrichtung	Besonders wichtige Einrichtung
„Sektoren besonders wichtiger Einrichtungen“ oder „Sektoren wichtiger Einrichtungen“ (Anlagen 1 oder 2)	„Sektoren besonders wichtiger Einrichtungen“ (Anlage 1)
➢ Ab 50 Mitarbeiter ODER ➢ Ab 10 Mio. € Jahresumsatz und Jahresbilanzsumme	➢ Ab 250 Mitarbeiter ODER ➢ Ab 50 Mio. € Jahresumsatz und 43 Mio. € Jahresbilanzsumme

Betroffenheitsprüfung: Schmankerl Paradies GmbH

- Firma produziert bayerische Feinkost auf höchstem kulinarischen Niveau
- 40 Angestellte
- Jahresumsatz 7 Mio. €
- Jahresbilanzsumme 5 Mio. €
- Sektor ist reguliert
- Aber Anzahl der Angestellten und Jahresumsatz sind zu niedrig

⇨ Unternehmen nicht von NIS-2 betroffen

Betroffenheitsprüfung: Bayerische Uhrenschnitzler AG

- Hersteller hochwertiger Uhren
- 20 Angestellte
- Jahresumsatz 55 Mio. €
  Jahresbilanzsumme 50 Mio. €

Sektor prüfen

Nr.	Sektor	Branche	Einrichtungsart
5.2.1	Verarbeitendes Gewerbe/Herstellung von Waren	Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen	Unternehmen, die eine der Wirtschaftstätigkeiten nach Abschnitt C Abteilung 26 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben

			Herstellung von sonstigen Metallwaren a. n. g.	2599
26			Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen	
	26.1		Herstellung von elektronischen Bauelementen und Leiterplatten	
		26.11	Herstellung von elektronischen Bauelementen	2610*
		26.12	Herstellung von bestückten Leiterplatten	2610*
	26.2		Herstellung von Datenverarbeitungsgeräten und peripheren Geräten	
		26.20	Herstellung von Datenverarbeitungsgeräten und peripheren Geräten	2620
	26.3		Herstellung von Geräten und Einrichtungen der Telekommunikationstechnik	
		26.30	Herstellung von Geräten und Einrichtungen der Telekommunikationstechnik	2630
	26.4		Herstellung von Geräten der Unterhaltungselektronik	
		26.40	Herstellung von Geräten der Unterhaltungselektronik	2640
	26.5		Herstellung von Mess-, Kontroll-, Navigations-u. ä. Instrumenten und Vorrichtungen; Herstellung von Uhren	
		26.51	Herstellung von Mess-, Kontroll-, Navigations-u. ä. Instrumenten und Vorrichtungen	2651
		26.52	Herstellung von Uhren	2652
	26.6		Herstellung von Bestrahlungs-und Elektrotherapiegeräten und elektromedizinischen Geräten	

https://ec.europa.eu/eurostat/de/web/products-manuals-and-guidelines/-/ks-ra-07-015

26.52 Herstellung von Uhren

Diese Klasse umfasst die Herstellung von Klein- und Großuhren, Zeitmessgeräten und ihren Bestandteilen.

Diese Klasse umfasst:

- Herstellung von Klein- und Großuhren aller Art einschließlich Armaturbrettuhren
- Herstellung von Gehäusen für Klein- und Großuhren, einschließlich Gehäusen aus Edelmetallen
- Herstellung von Zeiterfassungsgeräten und Geräten für das Messen, Aufzeichnen und die sonstige Anzeige von Zeitabständen mit Uhrwerk oder Synchronmotor, z. B.:
  - Parkuhren
  - Stechuhren
  - Datums-/Uhrzeitstempeln
  - Zeitschaltuhren
- Herstellung von Zeitschaltern und anderen Zeitauslösern mit Uhrwerk oder Synchronmotor:
  - Zeitschlösser
- Herstellung von Bauteilen für Uhren und Uhrwerke:
  - Uhrwerke aller Art für Klein- und Großuhren
  - Federn, Steine, Zifferblätter, Zeiger, Brücken und sonstige Teile
  - Gehäuse für Klein- und Großuhren aus allen Materialien

Diese Klasse umfasst nicht:

- Herstellung nichtmetallischer Uhrbänder (Stoff, Leder, Kunststoff) (s. 15.12)
- Herstellung von Uhrbändern aus Edelmetallen (s. 32.12)
- Herstellung von Uhrbändern aus unedlen Metallen (s. 32.13)

Sektor prüfen

Nr.	Sektor	Branche	Einrichtungsart
5.2.1	Verarbeitendes Gewerbe/Herstellung von Waren	Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen	Unternehmen, die eine der Wirtschaftstätigkeiten nach Abschnitt C Abteilung 26 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben

Prüfung der Size-cap-Regel

Wichtige Einrichtung	Besonders wichtige Einrichtung
„Sektoren besonders wichtiger Einrichtungen“ oder „Sektoren wichtiger Einrichtungen“ (Anlagen 1 oder 2)	„Sektoren besonders wichtiger Einrichtungen“ (Anlage 1)
➢ Ab 50 Mitarbeiter ODER ➢ Ab 10 Mio. € Jahresumsatz und Jahresbilanzsumme	➢ Ab 250 Mitarbeiter ODER ➢ Ab 50 Mio. € Jahresumsatz und 43 Mio. € Jahresbilanzsumme

Betroffenheitsprüfung: Bayerische Uhrenschnitzler AG

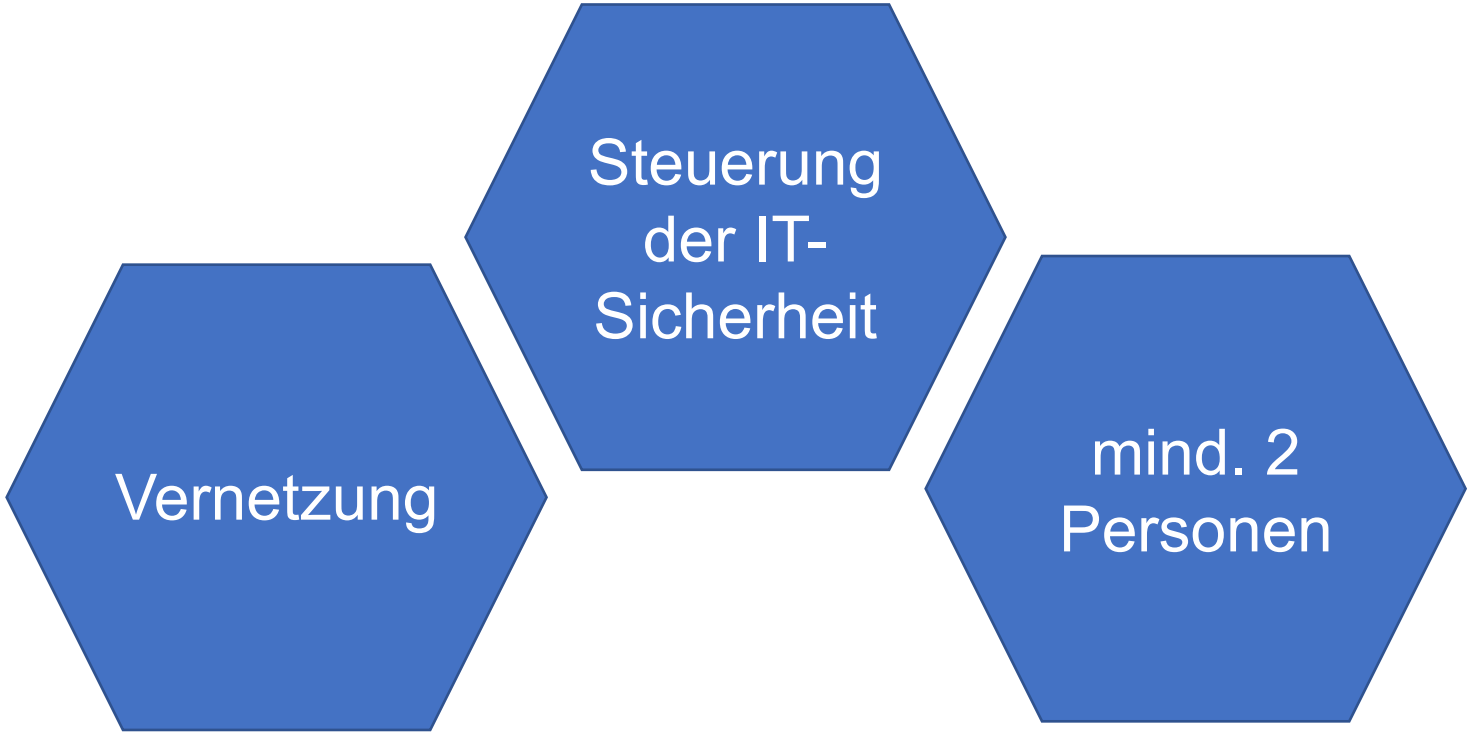
- Hersteller hochwertiger Uhren
- 20 Angestellte
- Jahresumsatz 55 Mio. €
  Jahresbilanzsumme 50 Mio. €
- Sektor ist reguliert
- Jahresumsatz und Jahresbilanzsumme liegen über Schwellenwerten für „wichtige Einrichtungen“

⇨ Unternehmen von NIS-2 betroffen: Wichtige Einrichtung

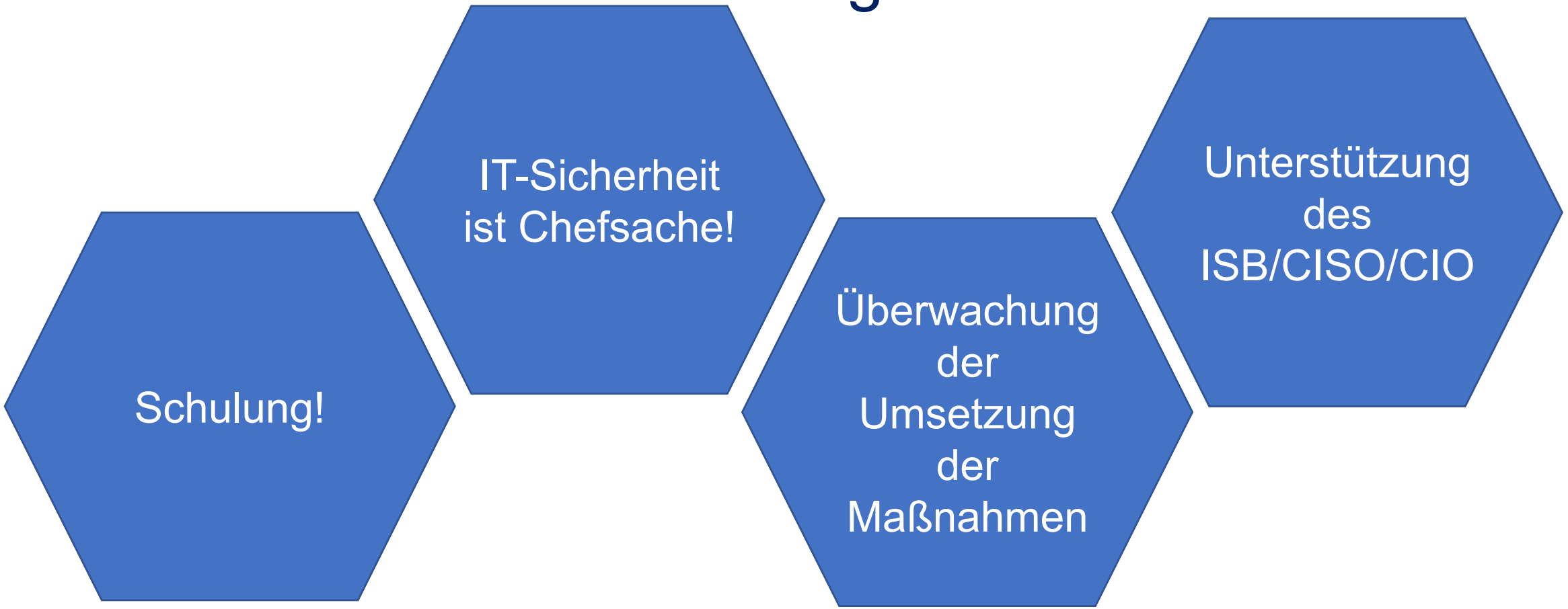
Welche Schritte müssen Sie ergreifen?

- Stadtwerke Wolkenkuckucksheim sind nach NIS-2 eine besonders wichtige Einrichtung.
- Die Geschäftsleitung hat festgestellt, dass sie von NIS-2 betroffen ist und möchte sich und ihr Unternehmen nun bestmöglich auf die kommende Regulierung vorbereiten
- Was muss hierbei beachtet werden?

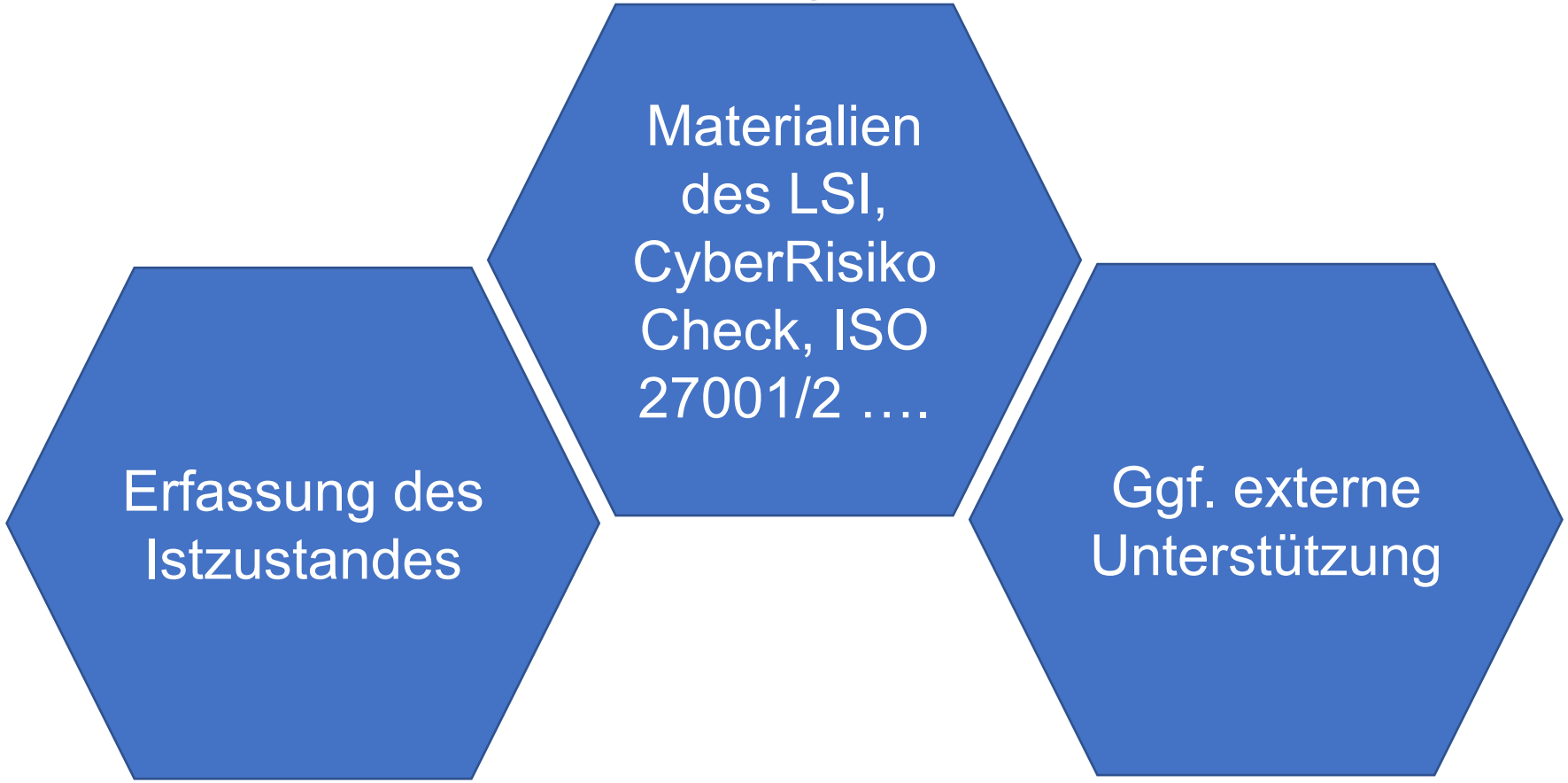
Verantwortlichkeiten festlegen



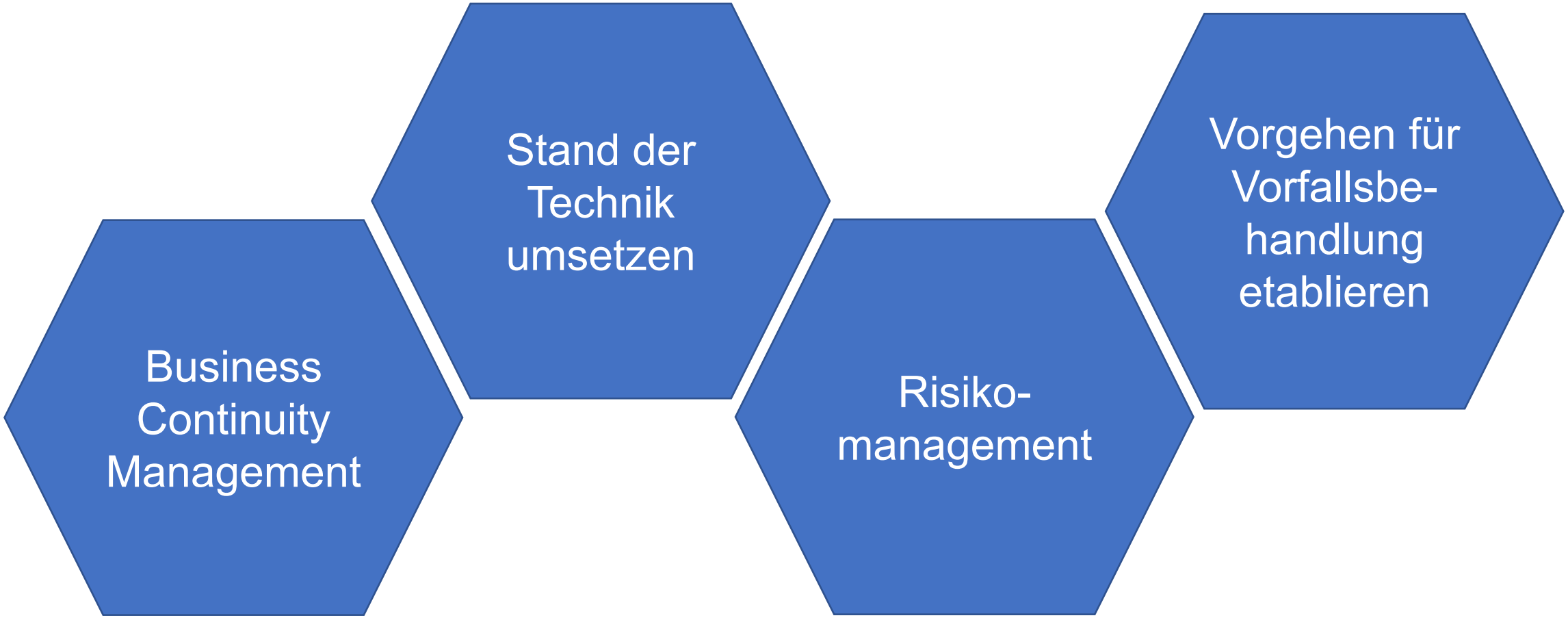
Pflichten der Geschäftsleitung



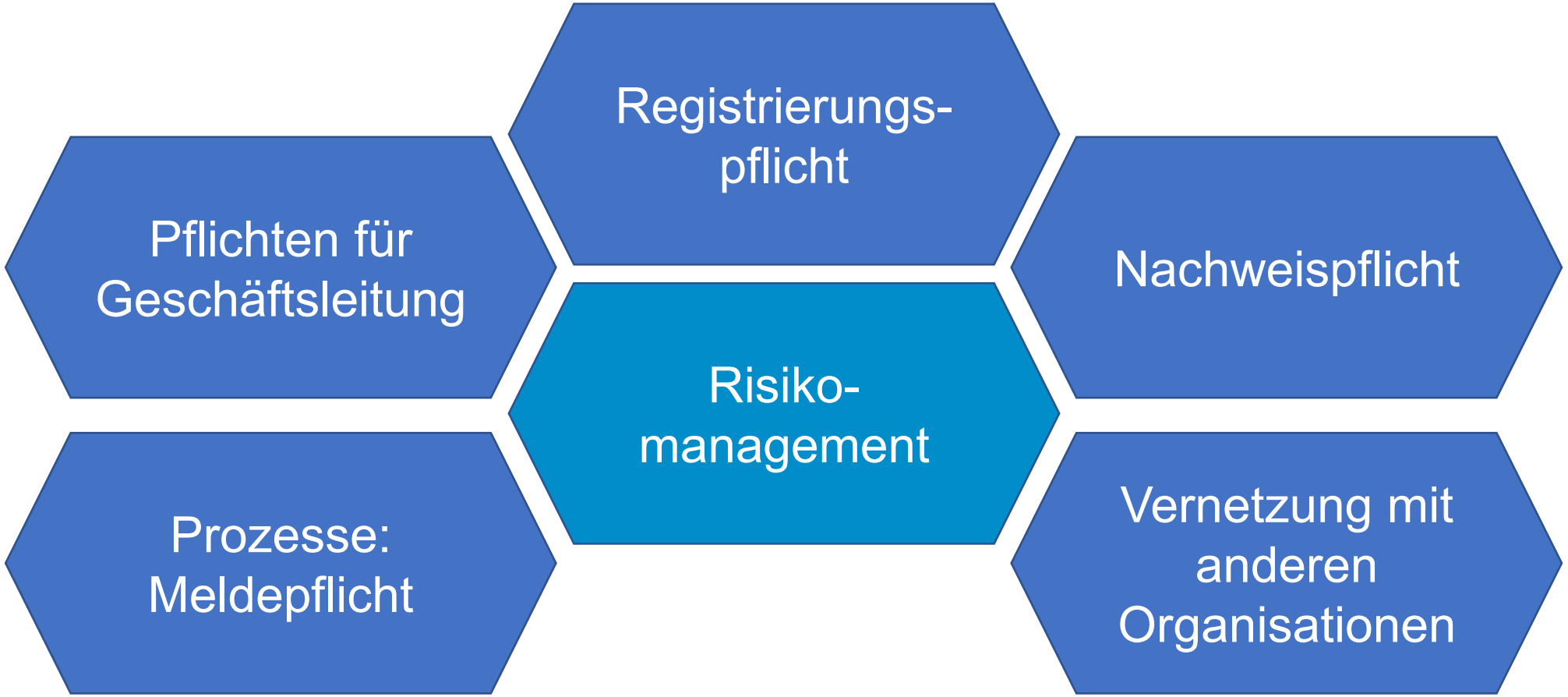
Ermittlung der aktuellen Informationssicherheitslage



Informationssicherheit erhöhen



Vorbereitung auf NIS-2



Kontaktdaten

Für Ihre Anliegen steht Ihnen gerne zur Verfügung:

Landesamt für Sicherheit in der Informationstechnik
LSI Referat 32 – „IT-Sicherheit öffentlicher KRITIS-Betreiber“
Keßlerstraße 1
90489 Nürnberg

Telefon: 0911 21549-525

Mail: beratung-kritis@lsi.bayern.de

Web: lsi.bayern.de