NIS2

Modell und Umsetzungspraxis – ein Blick in die betriebliche Wirklichkeit

Anton Sepper, CISO Wiener Linien

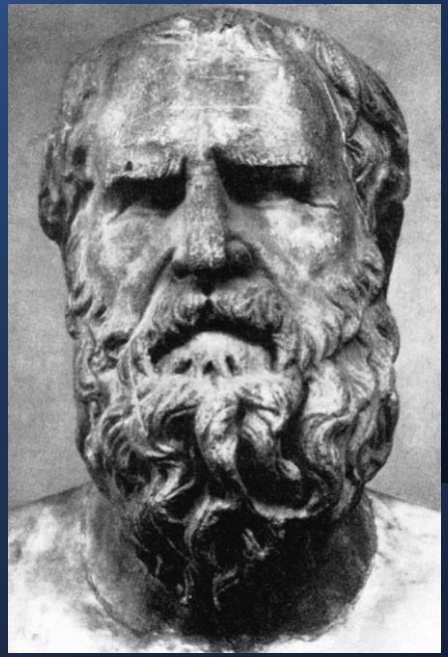
Prolog

Was ist Sicherheit?

Prolog

Sicherheit = Kontrolle über Veränderung

Prolog



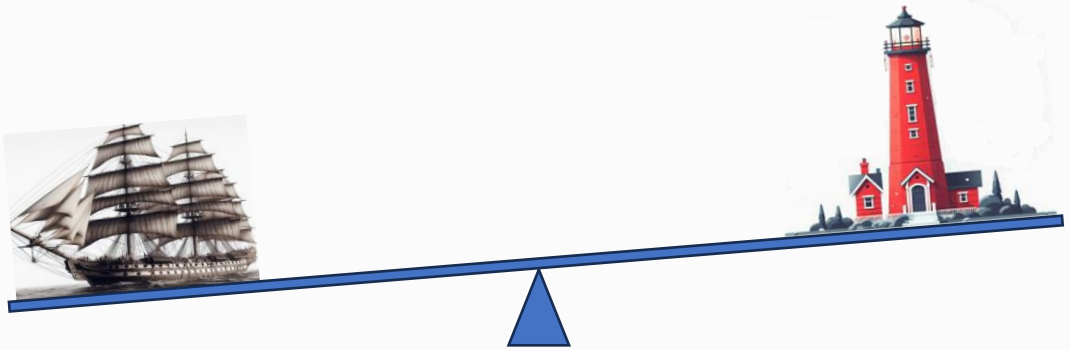
Heraklit von Ephesos, um 500 v. Chr.

Veränderung akzeptieren und vernünftig steuern generiert Sicherheit

πάντα ῥεῖ – alles fließt

Prolog

Dazu ist es wichtig, ein passendes Verhältnis zwischen Veränderung und Beharrung zu finden.



Kann Veränderung Begeisterung auslösen?

Kommt darauf an, ob sie …

⇨ verstanden wird

⇨ gesteuert werden kann

⇨mit Vorteilen einhergehend begriffen werden kann

Erfahrung mit Veränderung zu NISG und NIS2 +/-

Vorteile

- Einfach zu verstehende, praktikable Systematik
- Sehr gute Übersicht
- Die Ziele kommen mitten ins Unternehmen hinein
- Eindeutige Identifizierung der „Kronjuwelen“
- Erhöhte Nachvollziehbarkeit des Geschehens, bessere Steuerung von Veränderung
- Universell verwendbare Ergebnisse
- Nach Etablierung WENIGER Aufwand

Nachteile

- Mehr Aufwand:

  Arbeit, Personal, Aus- und Weiterbildung, Kompetenzbildung, Arbeitsmittel, Prozesse, Hard- und Software, Prüfungen und Audits, Verwaltung, sonstige Ressourcen

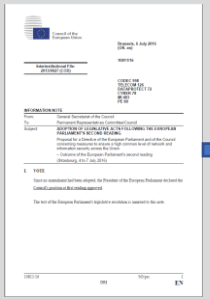
- Veränderung per se, wenn man sie ausschließlich als Bedrohung empfindet


NIS2

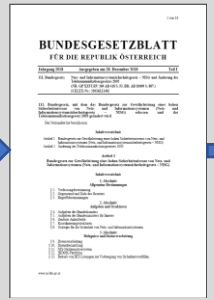
NIS2: Das Regelwerk - ein bisschen Statistik

NIS2: Das Regelwerk - Genesis

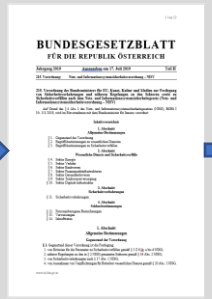
EU-Richtlinie



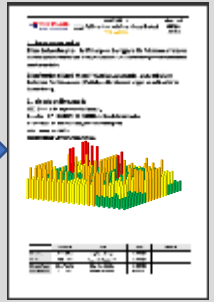
NIS-Gesetz



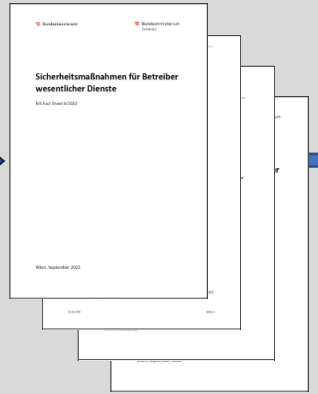
NIS-Verordnung



BIA & RM



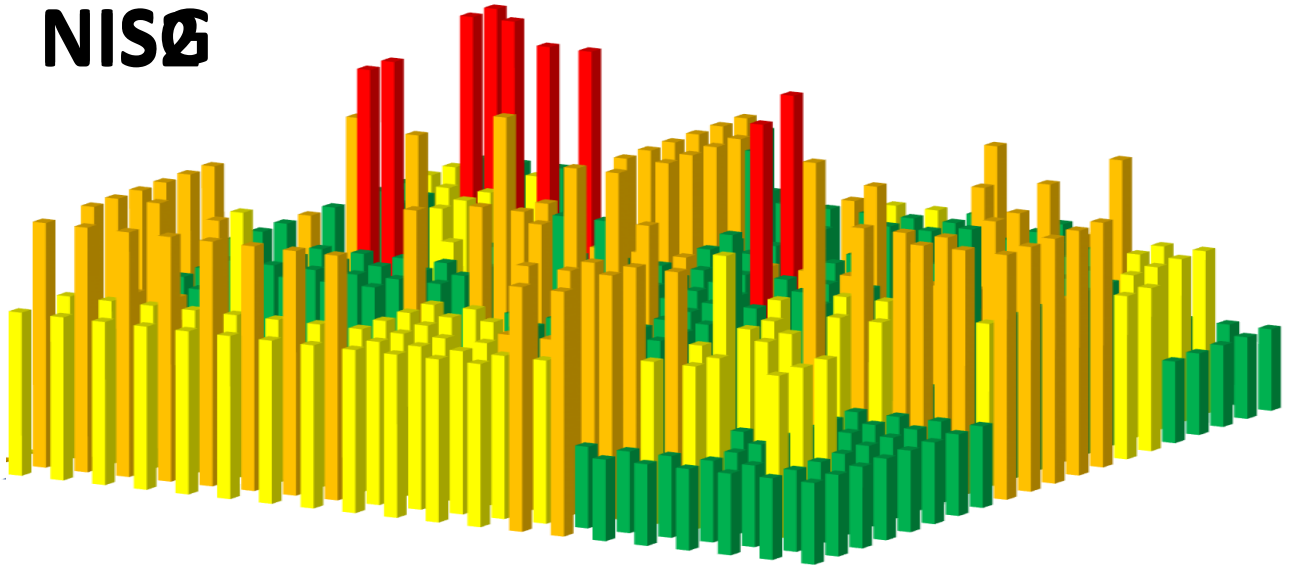
Factsheets



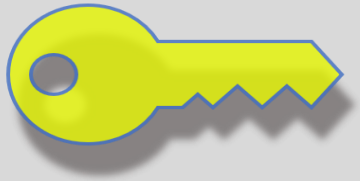
ISO 27001

ISMS

Umstellung auf NIS2 – Methodik und Ausblick



NIS2
der harte Kern



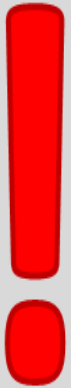
- NIS2 zeichnet eine **gesamtheitliche Strategie** vor
- Ihr Zentrum ist ein **angemessenes, aktuelles Risikomanagement**

NIS2 – Fokus Risikomanagement

Ein Zitat aus den Entwürfen zum Regelwerk:

„Hinsichtlich der von den Einrichtungen betriebenen Dienste können diese Pflichten jedoch ***unterschiedlich ausfallen****, wie ein Blick auf das* ***risikobasierte Vorgehen*** *[…] zeigt.“*

NIS2 – Fokus Risikomanagement



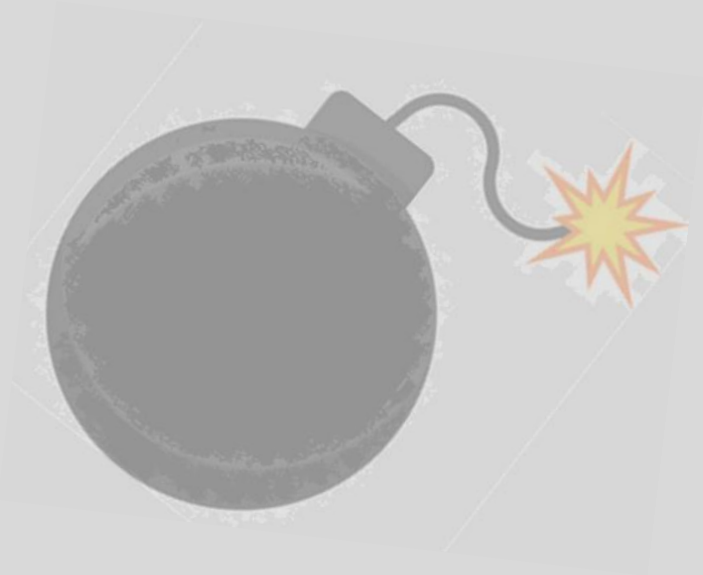
*Um dieses „**unterschiedlich ausfallen“** ökonomisch wirksam werden zu lassen, muss man sein Unternehmen, dessen Dienste, Assets und seine Prozesswelt **sehr gut kennen**. Andernfalls können die notwendigen Zuordnungen zu Kritikalität und Risikomanagement nicht argumentativ einwandfrei getroffen werden.*

Botschaft angekommen:

Irgendetwas mit Risiko - aber wie jetzt genau weiter???

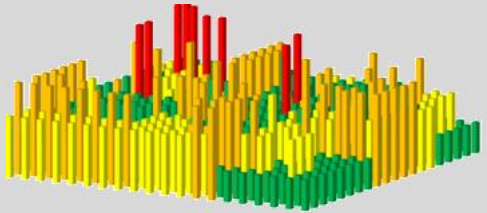
Das Wichtigste zuerst – ein Appell

- Verlieren Sie keine Zeit!
- Warten Sie nicht auf das Gesetz!
- Die wesentlichen Grundlagen zur IS sind längst etabliert, hinlänglich bekannt und allgemein zugänglich – packen Sie es an! Am besten noch heute!



Königsdisziplin Risikomanagement

1. Übersicht über den „Organismus Unternehmen“ erstellen
2. Kritikalitätsbeurteilung der erbrachten Dienste
3. Feststellung der bestehenden Risiken



4. Behandlung der Risiken nach den gewonnenen Erkenntnissen

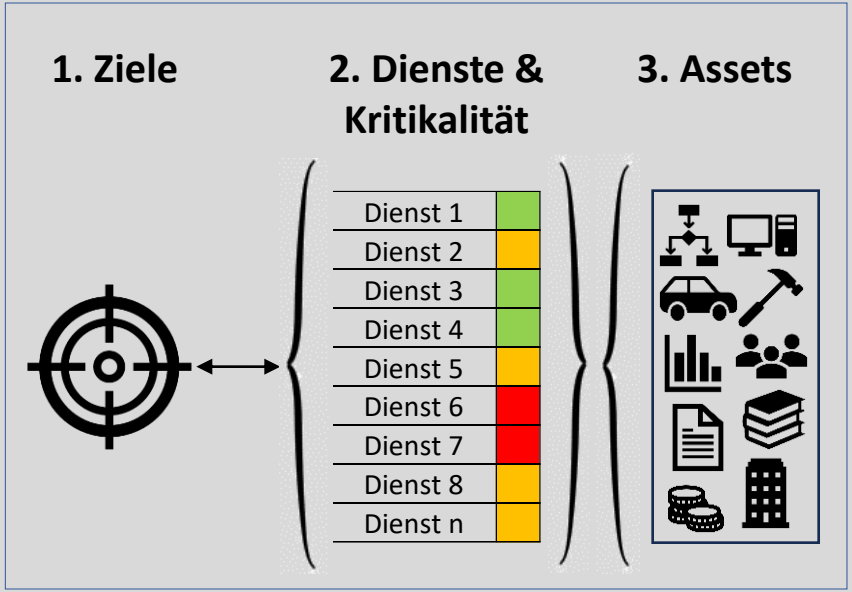
Königsdisziplin Risikomanagement

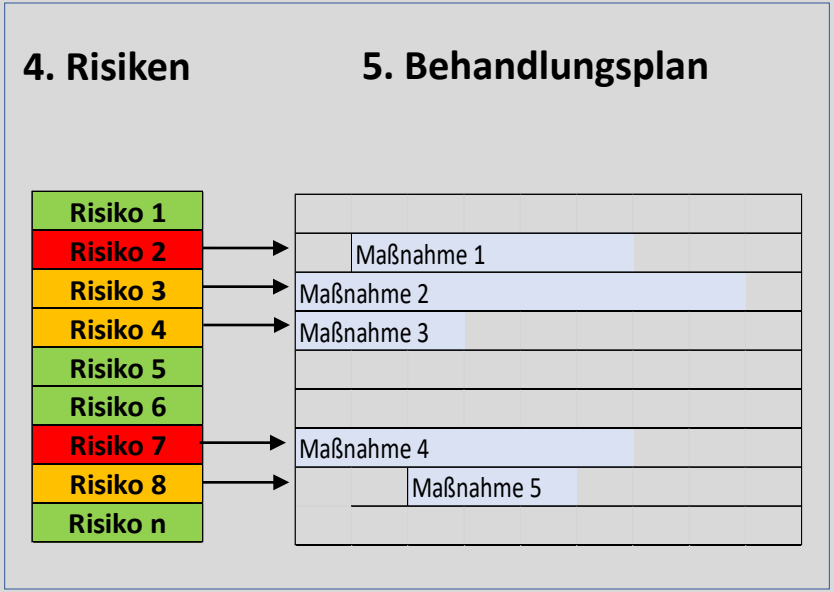
Stimmt, aber eins nach dem anderen…

1. **Ziele**
2. **Dienste** zur Zielerreichung -> Übersichtsbild
3. **Kritikalität**sbewertung der Dienste ⇨ **BIA**
4. **Assets** zur Realisierung der Dienste
5. **Eintrittswahrscheinlichkeit** eines Ausfalls ⇨ **RM**
6. **Behandlungsplan** zur Risikosteuerung
7. **Notfallmaßnahmen** zur Aufrechterhaltung der Dienste ⇨ **BCM**

Königsdisziplin Risikomanagement

Nochmals in der Abfolge dargestellt





Projekt Teil 1

Projekt Teil 2

Königsdisziplin Risikomanagement

Anwendung auf das Lieferantenmanagement

Königsdisziplin Risikomanagement

2. Kritikalitätsbewertung

1. Lieferantenverzeichnis

3. Risikobewertung

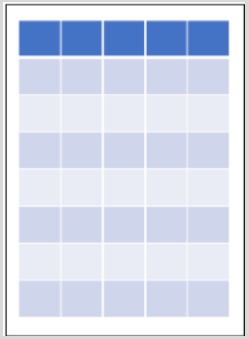
4. Maßnahmen

Angewendet aufs Lieferantenmanagement:

1. **Ziele**
2. **Dienste** zur Zielerreichung -> Übersichtsbild
3. **Kritikalität**sbewertung der Dienste ⇨ **BIA**
4. **Assets** zur Realisierung der Dienste
5. **Eintrittswahrscheinlichkeit** eines Ausfalls ⇨ **RM**
6. **Behandlungsplan** zur Risikosteuerung
7. **Notfallmaßnahmen** zur Aufrechterhaltung der Dienste ⇨ **BCM**

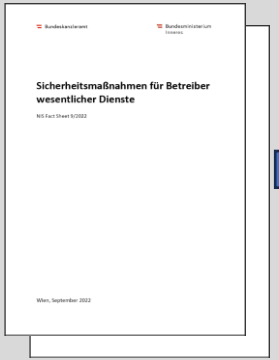
Lieferanten als Asset

Lieferanten-verzeichnis



1. Lieferantenverzeichnis
2. Kritikalitätsbewertung
3. Risikobewertung
4. Maßnahmen

1. Factsheet NISG
2. Anlage 3 NIS2



Lieferanten als Asset

1. Factsheet NISG

2. Umgang mit Dienstleistern, Lieferanten und Dritten

Hinweis: Es macht hinsichtlich der Prüfanforderungen keinen Unterschied, ob Netz- und Informationssysteme, von denen der wesentliche Dienst abhängt, vom jeweiligen Betreiber selbst oder von einem Dienstleister betrieben werden. Eine Überprüfung durch eine qualifizierte Stelle ist jedenfalls notwendig.

Wenn das bei oder von einem Dienstleister betriebene Netz- und Informationssystem durch eines beim jeweiligen Betreiber betriebene Netz- und Informationssystem soweit ersetzt werden kann, dass der Ausfall bzw. die Nichtaufrechterhaltung der Integrität des Dienstleisters keine erheblichen Auswirkungen auf den wesentlichen Dienst hat, ist dieses Netz- und Informationssystem des Betreibers und das diesbezügliche Konzept bzw. der diesbezügliche Prozess einer Überprüfung durch eine qualifizierte Stelle zu unterziehen.

2.1 Beziehungen mit Dienstleistern, Lieferanten und Dritten

NIS-Verordnung:
Anforderungen an Dienstleister, Lieferanten und Dritte für den Betrieb von, einen sicheren Zugang zu und Zugriff auf Netz- und Informationssysteme sind festzulegen und periodisch zu überprüfen.

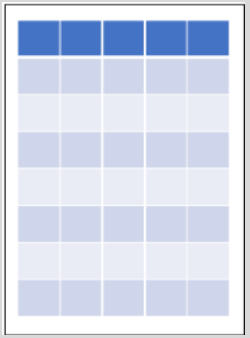
Der Betreiber erstellt ein Gesamtbild seines Ökosystems, einschließlich Dienstleister und Lieferanten mit vertraglichen Beziehungen sowie Dritter, insbesondere solcher, die Zugang zu den Netz- und Informationssystemen haben oder diese verwalten.

2. Anlage 3 NIS2

7.	**Sicherheit von Lieferketten**
a.	Richtlinie zur Sicherheit von Lieferketten
b.	Lieferantenverzeichnis

Lieferanten als Asset

Lieferanten-verzeichnis



1. Lieferantenverzeichnis
2. Kritikalitätsbewertung
3. Risikobewertung
4. Maßnahmen

Factsheet NISG Anhang 3 NIS2

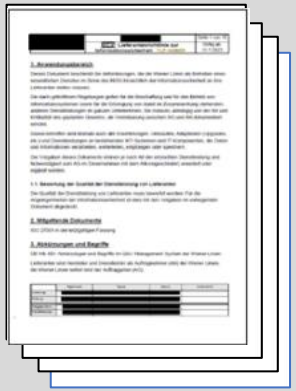
Behandlung der Lieferanten

Prüfungstypen im Lieferantenmanagement	Kurzbe-zeichnung
Einmaliges Sicherheitsgespräch	ES
Regelmäßiges Sicherheitsgespräch	RS
Selbstauskunft	SA
Lieferantenaudit des AG beim AN	LI
Beauftragtes Lieferantenaudit durch befugte Dritte	LE
Zertifizierung nach einschlägigem Regelwerk	ZT

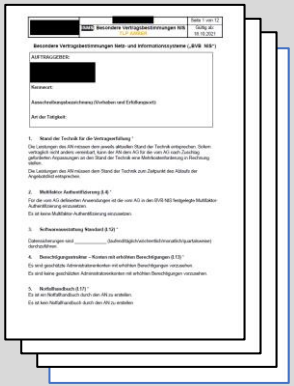
Lieferantenmanagement – Etablierung im Unternehmen

Lieferanten als Asset – zwei wichtige Dokumente:

1. **Lieferantenrichtlinie**



2. **Besondere Vertragsbestimmungen**



RM-Ergebnis als Ausgangslage

- Behandlungsplan erstellen und umsetzen
- Notfallpläne erstellen und erproben
- Prozesse und Abläufe prüfen und aktuell halten
- Dokumentieren, dokumentieren, dokumentieren!
- NIS2 gelassen entgegensehen

RM-Ergebnis als Ausgangslage

- Behandlungsplan erstellen und umsetzen
- Notfallpläne erstellen und erproben
- Prozesse und Abläufe prüfen und aktuell halten
- Dokumentieren, dokumentieren, dokumentieren!
- NIS2 gelassen entgegensehen

NIS2 – Vorbereitung

Kann das alles auch automatisiert erledigt werden ?

- Es gibt Produkte, die dabei unterstützen
- **Sie ersetzen nicht den Einsatz von sachkundigen Personen**
- Die Verwendung solcher Erzeugnisse ist immer auch eine Frage wirtschaftlicher Betrachtung
- NIS2 ist eine exzellente Gelegenheit, sein Unternehmen noch besser kennen zu lernen

Erfahrungen aus der Praxis

Wie beginnen?

1. Erstellen Sie ein **EINFACHES**, sequenzielles und für alle Beteiligten aus ihrer spezifischen Perspektive heraus verständliches **Grundkonzept**, das in ein strategisches Projekt übergeführt werden kann.
2. Bilden Sie dieses Grundkonzept **präsentierfähig** ab.
3. Involvieren Sie frühzeitig die zur Etablierung des anstehenden **Kulturwandels** notwendigen **Rollen** quer durch Ihr Unternehmen!
4. Abstimmung mit der obersten Leitung. Information alleine genügt nicht, es bedarf der eindeutigen und allgemein wahrnehmbaren **Willenskundgebung der Unternehmensleitung** zur Umsetzung, z.B. in Form eines Projektauftrags.
5. Skizzieren Sie bereits von Anbeginn an die von den OE Ihres Unternehmens **selbständig zu leistenden Anteile** am Gesamtprojekt – es muss verstanden werden, dass die OE nicht „für das Projekt“ arbeiten, sondern für ihre eigenen Interessen im Sinne der Unternehmensziele.

Weiter auf dem Weg

6. Vermeiden Sie den gravierenden **Kardinalfehler** zu glauben, dass man eine kompetente Person einstellen oder zukaufen kann, die dann – ohne intensive Einbeziehung des Unternehmens - „das alles für uns erledigt“. Das funktioniert nicht, zeugt aber von völligem Unverständnis für die Situation.

7. Finden Sie sich damit ab, dass vom vor Ihnen liegenden Projekt alle OE und **alle Personen**, eingeschlossen Ihre Kunden und Lieferanten, betroffen sein werden, wenn auch in unterschiedlichem Detaillierungsgrad.

8. Unterschätzen Sie nicht die vorherrschende **innerbetriebliche Dynamik**, lernen Sie sie kennen. Legen Sie Ihr Augenmerk auf informelle Kontakte, auf verdeckten Gleichklang oder Gegensätze zwischen den OE und den handelnden Personen. Das lohnt sich, denn diese Fakten beeinflussen das Gesamtgeschehen meist viel stärker, als auf den ersten Blick sichtbar ist.

9. Haben Sie Geduld, rechnen Sie mit Fehlern und Bremsstrecken, verlieren Sie nicht die Nerven, bleiben Sie **freundlich** aber in der Sache **konsequent** dran.

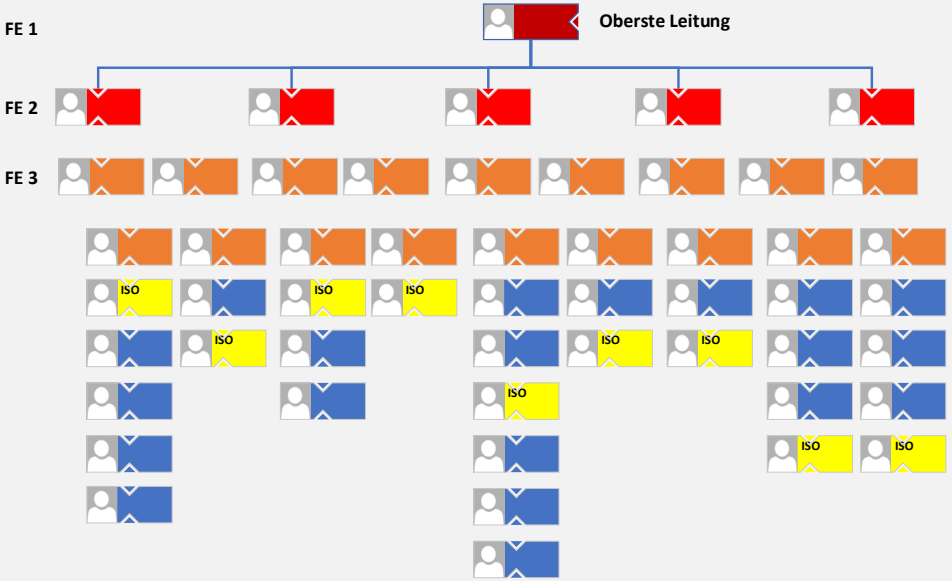
Weiter auf dem Weg

10. Achten Sie darauf, dass Sie die Projektinhalte in “kleinen Dosen” mit großzügiger Zeitplanung **in jeder OE** durchexerzieren.

11. Halten Sie sich vor Augen, dass die von Ihnen „für NIS“ etablierte Systematik, wenn Sie das klug anlegen, auch als ausgezeichnete Grundlage zur Bewältigung noch nachfolgender Regulative wie z.B. des Themenkomplexes *Resilienz für kritische Infrastrukturen* dienen kann.

12. Wenn Sie davon nicht direkt betroffen sind, weil Sie mit Ihrem Unternehmen unter die Schwellwerte zur Anwendung des neuen NIS2-Gesetzes fallen, sollten Sie sich dennoch mit der Materie beschäftigen und, wo es notwendig ist, mitziehen. Es ist recht wahrscheinlich, dass Sie Lieferant von kritischen oder wichtigen Einrichtungen im Sinne des Gesetzes sind oder werden und können damit einen erheblichen Marktvorteil erringen. Die betroffenen Unternehmen müssen nämlich in ihrem Lieferantenmanagement entsprechende Rücksichten treffen.

Die wichtigsten Mitspieler auf einen Blick



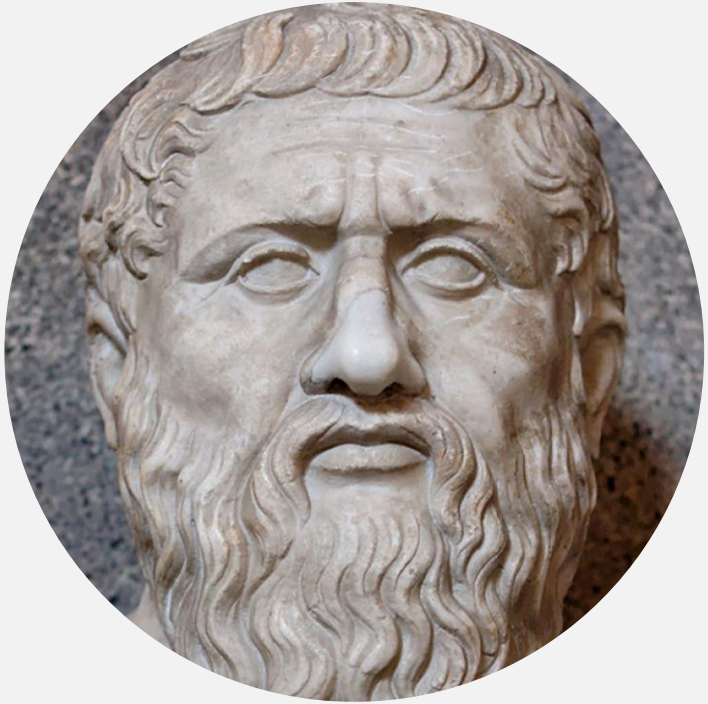
Zuviel der Worte – geht das auch kürzer?

$$\forall x \left(R(x) \wedge M \in R \right) \Rightarrow C$$

Wenn **alle** Elemente “x” die Eigenschaft “R” haben (d.h. dem Risikomanagement unterworfen sind) und “M” (laufende Maßnahmenplanung) ein Teil von “R” ist, dann folgt daraus, dass “C”(auf gutem Weg zur Compliance zu NIS2) ebenfalls wahr ist.

Zum Schluss ein bisschen Philosophie

- Wieviel Technik, Wissen und andere Ressourcen Sie auch aufwenden werden, zuletzt sind es immer **Menschen**, die handeln und es sind Menschen, für die das Ganze überhaupt getan wird.
- Und so gut Sie Ihre **Assets und Ihr Business** auch kennen mögen, so gut sollten Sie die handelnden **Personen** und ihre Motive und Bedürfnisse kennen.
- Wenn Sie dann auch nicht vergessen, dass **von Menschen kreierte Systeme** immer **menschliche Grundzüge** eingeschrieben haben, die wir alle zur Genüge kennen, können Sie das Ausmaß an Störgrößen für Ihr Vorhaben gering halten.



Gutes Gelingen!