NIS-2 – viele Anforderungen, wenig Neues

Know-how to go

12.6.2025

Andre Windsch

Who am I

Andre Windsch
Senior Expert bei der HiSolutions AG

M. SC Informatik

Beratung & Prüfung im Kontext Cybersicherheit mit Schwerpunkt auf regulatorischen Anforderungen:

- (IT-) Risikomanagement
- Aufbau von Management Systemen (Informationssicherheit, Business Continuity & Krise, integrierter Aufbau)
- „angemessene & wirksame“ / „effektive & effiziente“ Umsetzung
- Interne & externe Audits

NIS2 Pflichten

Registrierungspflicht (§33,§34)
- Bestimmung der eigenen Betroffenheit und Registrierung bei zuständiger Behörde (BSI, BBK, BNetzA oder BaFin)

Risikomanagement inkl. technischer und organisatorischer Maßnahmen (§30,§31)
- Umsetzung geeigneter, verhältnismäßiger, wirksamer, auf Stand der Technik, sowie Standards/Normen und Risikoexposition basierender TOM

Meldemechanismen inkl. Unterrichtungspflicht (§32)
- Vorgehen im Krisenfall, Identifikation von internen und externen Ansprechpartnern, interne Sicherheitsvorfalldefinition und -behandlung

Nachweispflicht (§39)
- über Risikomanagement, Einhaltung der Meldepflichten und Systeme zur Angriffserkennung* bspw. über Auditergebnisse, Prüfungen oder Zertifikate

Geschäftsleitungspflichten (§38)
- Umsetzung und Überwachung des Risikomanagements, Schulungspflicht für C-Ebene zu Risikomanagement und Sicherheit in der IT

kurz gesagt

- Umfassendes Anforderungen zur Informationssicherheit
- Ca. 30.000 Unternehmen betroffen
- Inklusion der Lieferkette
- Wenige Ausnahmen (in der Wirtschaft)
- Befugniserweiterung für BSI
- Empfindliche Strafen

Cybersicherheit: Risikomanagement

Umsetzung von **angemessenen** und **verhältnismäßigen** Maßnahmen in verschiedenen Themenbereichen

Kriterien

- Risikoexposition
- Größe der Einrichtung
- Umsetzungskosten
- Eintrittswahrscheinlichkeit
- Schwere von Sicherheitsvorfällen
- Gesellschaftliche / wirtschaftliche Auswirkungen

Themenbereiche

- Risiko Management
- Informationssicherheitsmanagement
- Asset Management
- Technische Sicherheit
- Personelle & organisatorische Sicherheit
- Notfall- & Krisen Management
- Lieferanten, Dienstleister und Dritte
- Vorfallerkennung und -bearbeitung

KRITIS: Aufwändigere Maßnahmen verhältnismäßig, wenn erforderlicher Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage steht

Für die Betrachtung wurden die „Implementation Guidance on … technical and methodological requirements of cybersecurity risk-management measures“ (ENISA) für spezielle IT-Dienste Anbieter genutzt

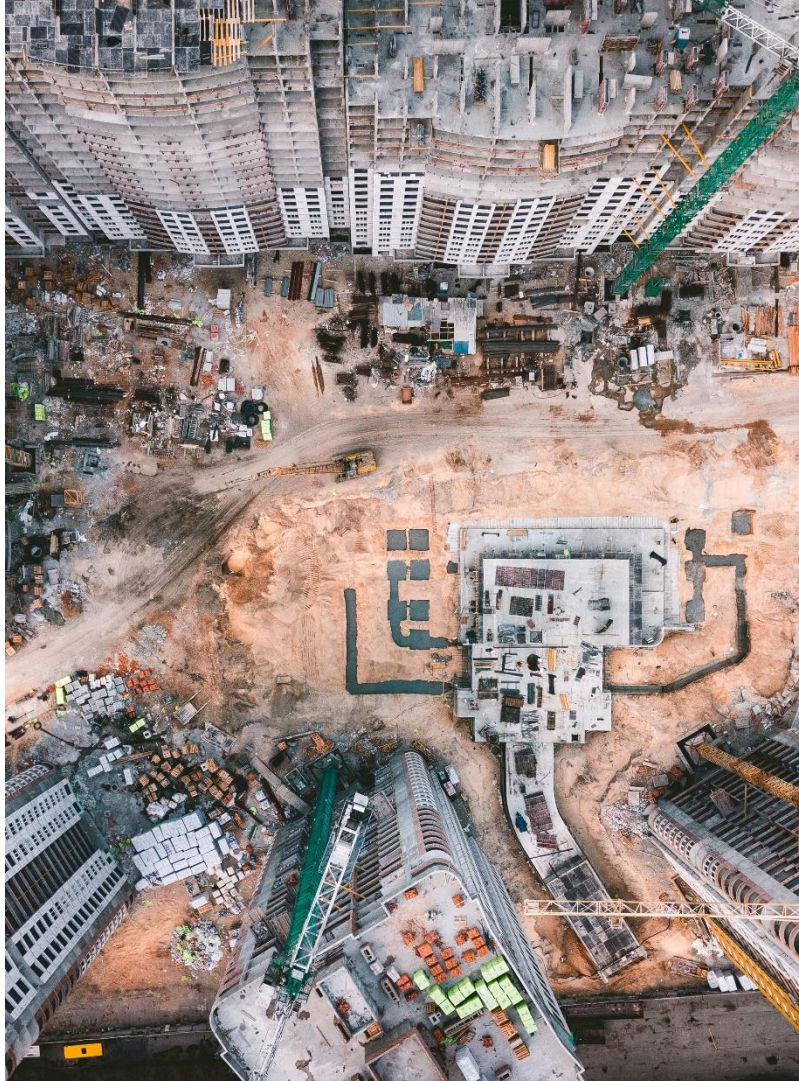
Übergreifende Anforderungsbereiche

1. Strukturen und Prozesse schaffen und dokumentieren („Management System“)

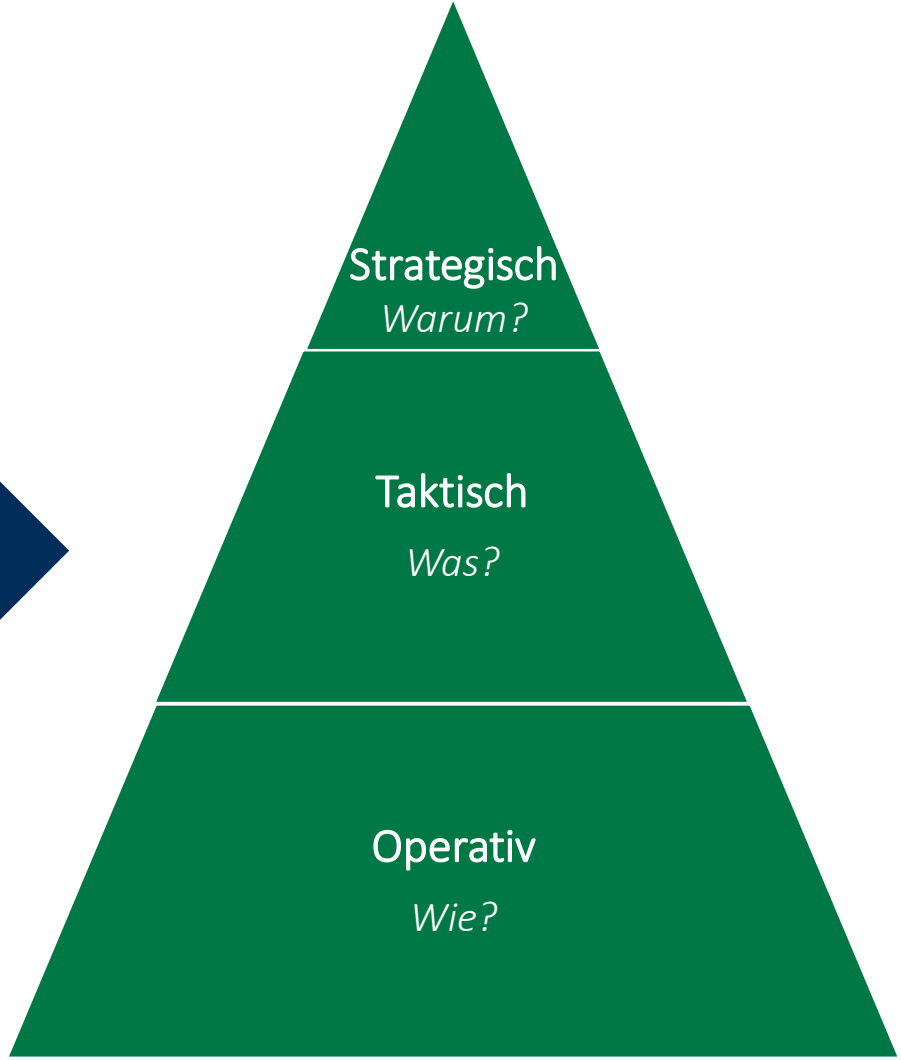
2. Operative Umsetzung

Gemeinsamkeit:

- Viele Anforderungen zielen auf ein Basis-Sicherheitsniveau, kein Hochschutz ab
- Durch „angemessen“ / „verhältnismäßig“ bzw. den Risiko-Bezug besteht entsprechender Spielraum in der Umsetzung



Typische Ebenen in Management Systemen

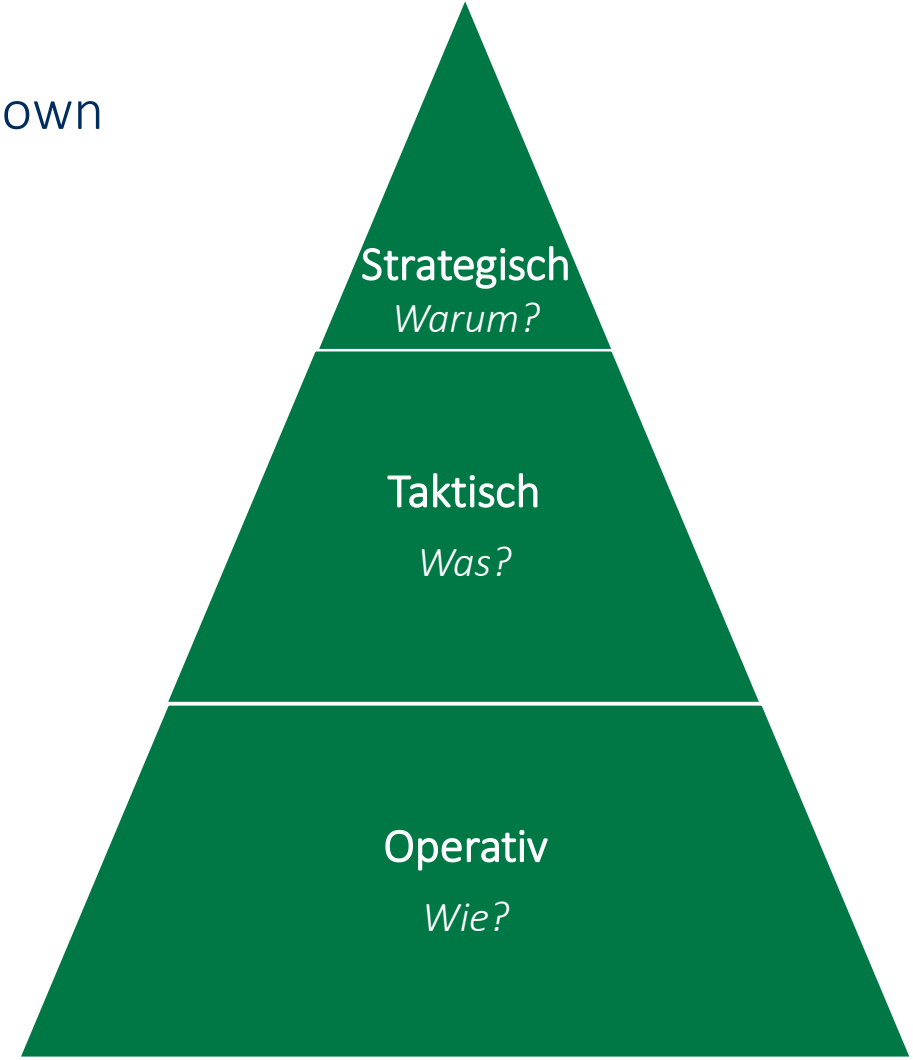


Umsetzung von Anforderungen – Top-Down

1. Definition der Ziele, Prozesse & Strukturen
2. Erstellen von Richtlinien & Konzepten
3. Umsetzung

Typische Vorteile
- Ganzheitlichere Betrachtung der Risiken
- Zielgerichtetere, ganzheitlichere Umsetzung
- Entscheidungen sind reproduzierbar
- Proaktiver

Typische Nachteile
- Viel Aufwand für formale Aspekte
- Hohe Dauer bis eine tatsächliche Umsetzung und damit Verbesserung erfolgt … und veraltet teilweise in der Erstellung
- „Kein Plan überlebt den ersten Feindkontakt“

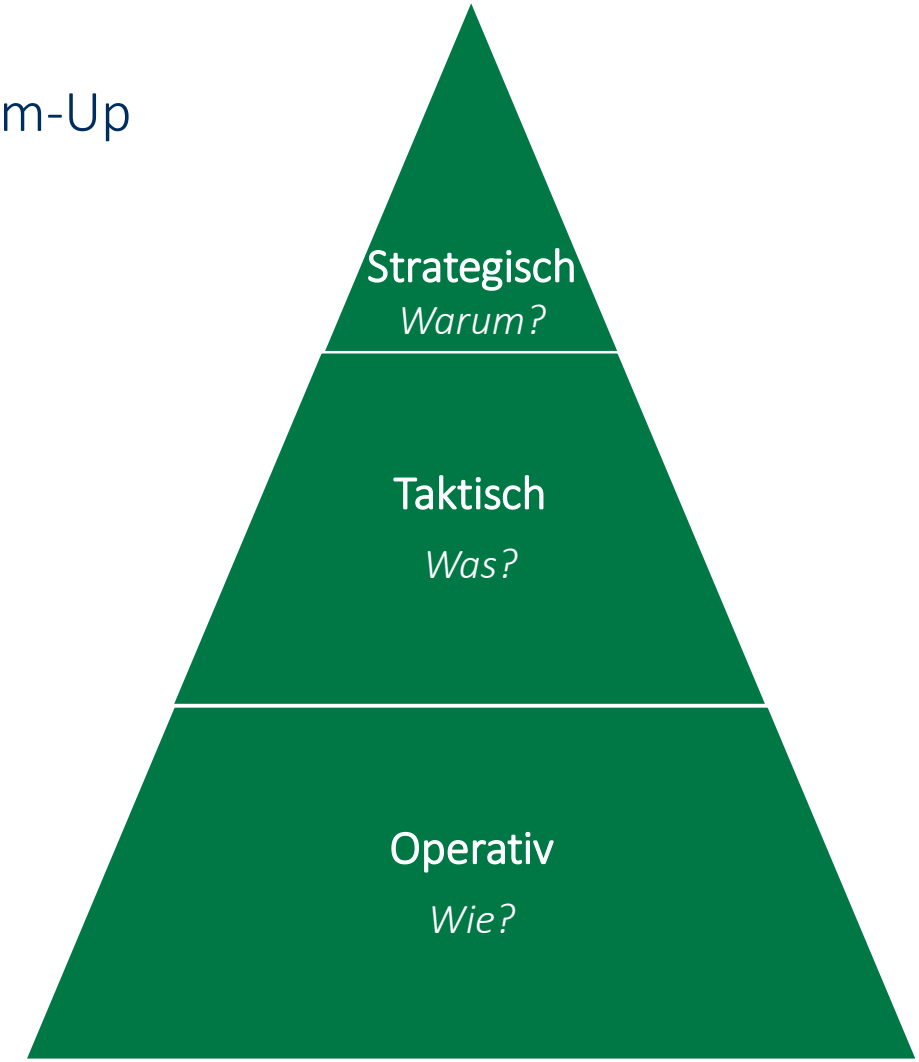


Umsetzung von Anforderungen – Bottom-Up

1. Umsetzen von Maßnahmen
2. / 3. „Aufschreiben“ und „kommunizieren“ was getan wird

Typische Vorteile
- Schnelle Verbesserung der Sicherheit
- Umsetzung näher an den aktuellen Gegebenheiten (Praxis-tauglicher)

Typische Nachteile
- Umsetzung & Bedarf passen oft nicht zusammen (zu viel oder zu wenig)
- Übersehen von relevanten Aspekten
- Umsetzungen greifen nicht ineinander
- Uneinheitliches Sicherheitsniveau
- Reaktives Vorgehen



Sicherheit – so stark wie ihr schwächstes Glied

Wieso geht es nicht ohne Management(systeme)

Klare Verantwortung & Entscheidungswege

Reproduzierbare Entscheidungen

Klare Ziele & Prioritäten

Einheitliches Sicherheitsniveau

Kontinuierliche Verbesserung

Explizit im Gesetz gefordert

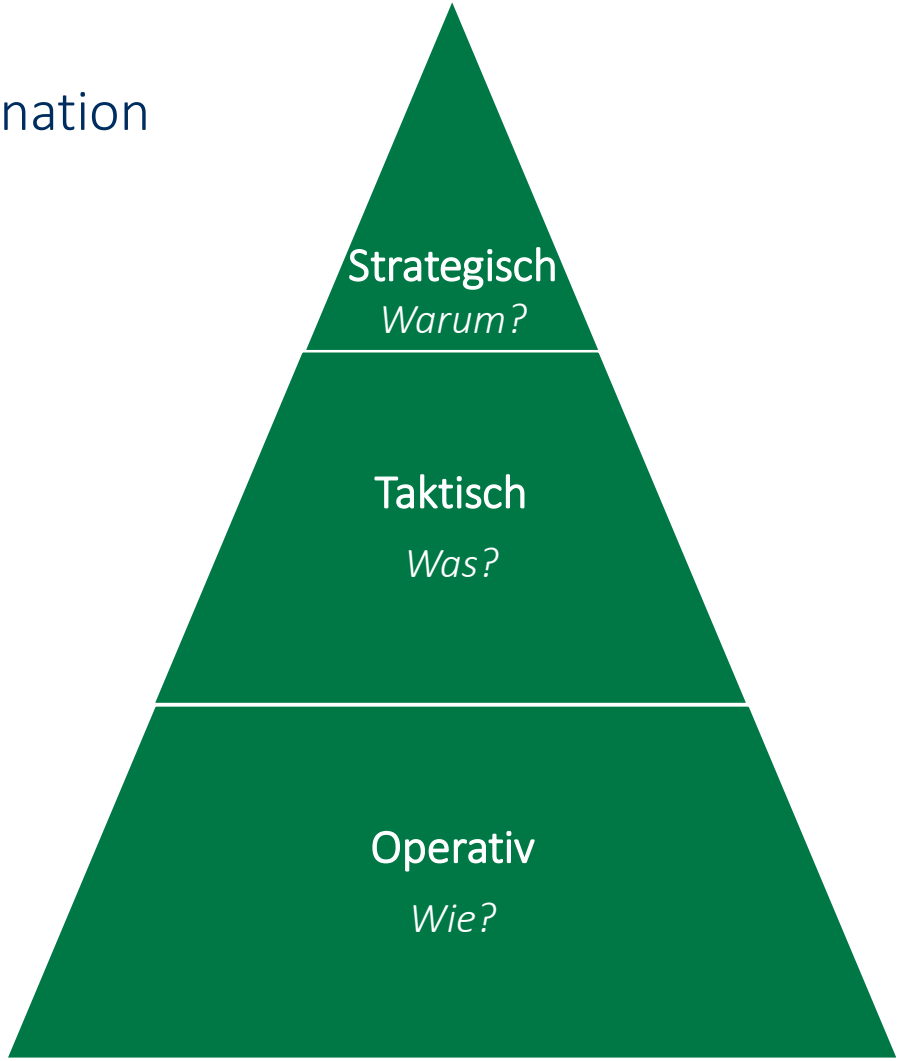
Wieso geht es nicht ohne Management(systeme)
… aber warum wird so oft die Praxistauglichkeit im Betrieb vergessen

Umsetzung von Anforderungen – Kombination

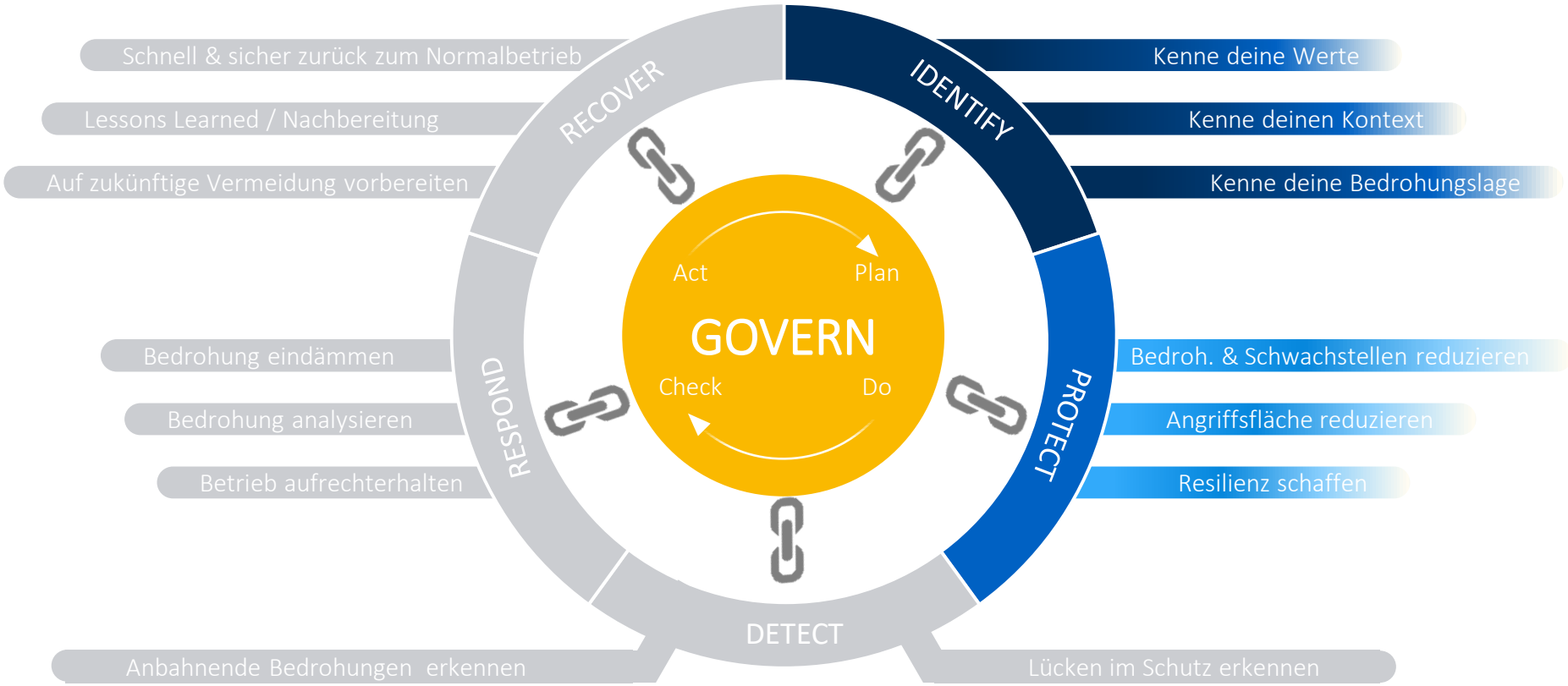
1. Definition der Ziele, Prozesse & Strukturen
   Umsetzung fehlender technischer & organisatorischer Basis-Themen (einfacher Plan)
2. Konzeption komplexerer / spezifischer Aspekte
3. Umsetzung der Konzepte

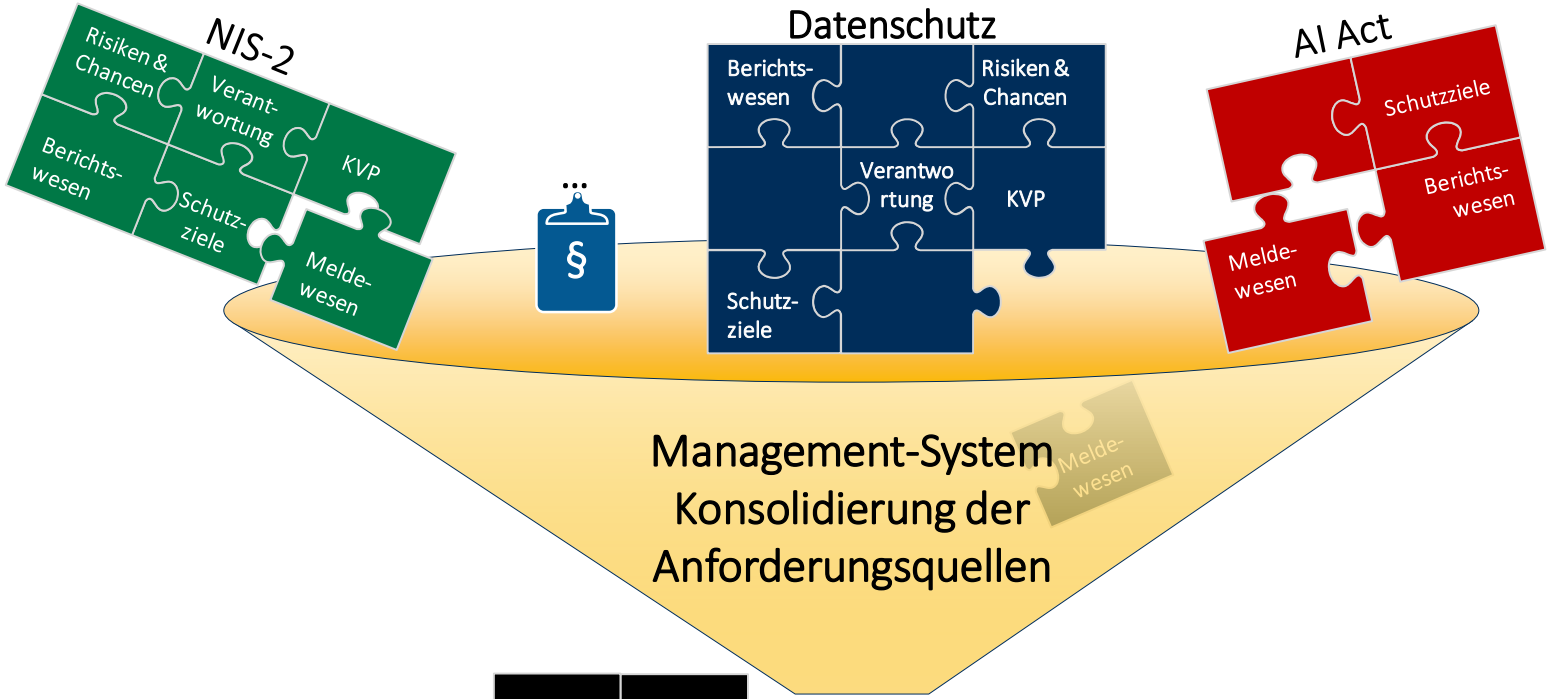
Wieso ist das sinnvoll?

- Grundlegende Aspekte der Informationssicherheit, technisch & organisatorisch sind nicht Betreiber-spezifisch
- Strategische Aspekte sowie die operative Umsetzung wird typischerweise durch andere Personen verantwortet und lässt sich parallelisieren

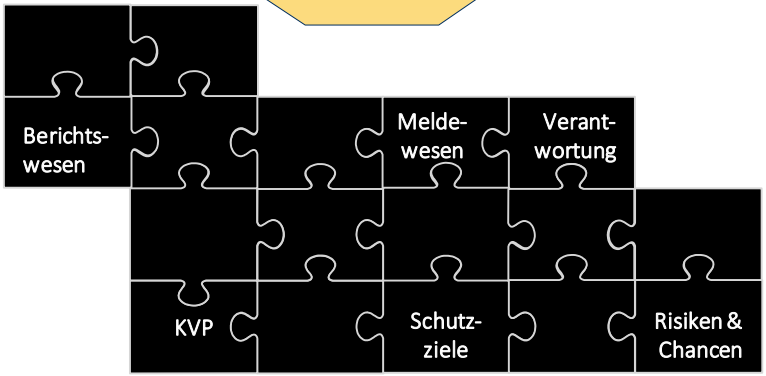


Start der Umsetzung





Interne & externe Vorgaben



Eigene Umsetzung

Fragen & Diskussionen

HISOLUTIONS

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com