Gesetzeslage aktuell

Know-how to go

12.6.2025

Manuel Atug

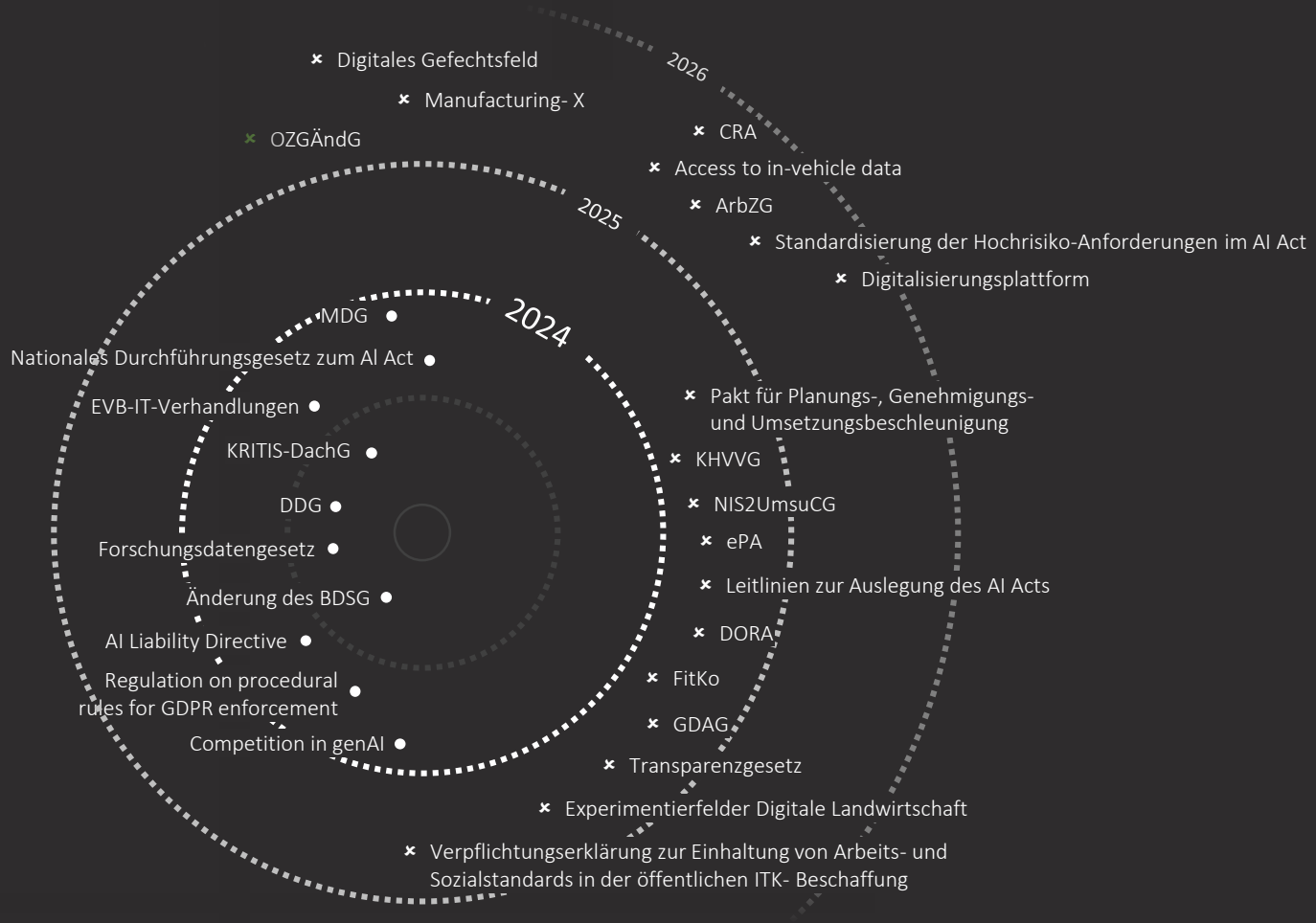
Who am I

Manuel Atug
Principal bei der HiSolutions AG

Diplom-Informatiker, Master of Science in Applied IT Security, Ingenieur

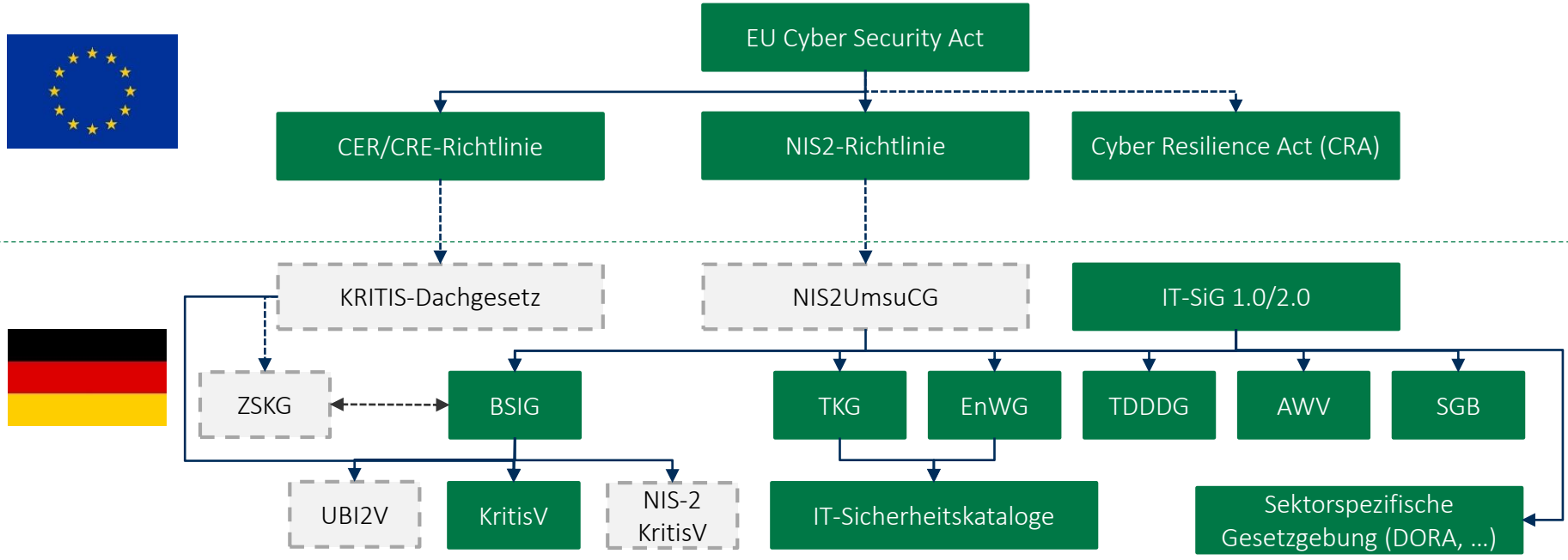
Begleitet KRITIS Betreiber bei Umsetzung der Anforderungen:
- ISMS, BCM, branchenspezifischer Stand der Technik (B3S)
- Notfall- und Continuity-Management

Prägender Berater des BSI § 8a BSIG und NIS-2



AI Act – Artificial Intelligence Act | **ArbZG** – Arbeitszeitgesetz | **BDSG** - Bundesdatenschutzgesetz | **CRA** - Cyber Resilience Act| **DDG** - Digitale-Dienste-Gesetz | **DORA** - Digital Operational Resilience Act | **ePA** - Elektronische Patientenakte | **FDG** – Forschungsdatengesetz | **FitKo** - Föderale IT- Kooperation | **GDAG** - Kompetenzen der Digitalagentur für Gesundheit | **KHVVG** - Krankenhausversorgungsverbesserungsgesetz | **KRITS-DachG** - KRITIS Dachgesetz | **MDG** - Mobilitätsdatengesetz | **NIS2UmsuCG** – Umsetzungsgesetzt zur Network & Information Security Richtlinie 2 | **OZGÄndG** - Gesetz zur Änderung des Onlinezugangsgesetzes

Übersicht zur Regulierungsstruktur



Grün: verabschiedet **Grau**: In Arbeit

So geht es weiter

EU NIS-2 Draft
16.12.2020
Veröffentlichung

EU NIS-2 Richtlinie
27.12.2022
Veröffentlichung

DE NIS2UmsuCG
(Gesetzesentwurf der Bundesregierung)
02.10.2024
Veröffentlichung

DE NIS2UmsuCG
04.11.2024
Anhörung im BT Innenausschuss

DE NIS2UmsuCG
Leak Version
vom 26.5.2025

Mögliches Inkrafttreten:
(Im 100 Tage Plan beabsichtigt)

Noch in 2025?

Nationale Umsetzungsfrist
18.10.2024
Per EU-Vorgabe

Deadline Registrierungspflicht
+ 3 Monate
(außer Betreiber kritischer Anlagen, diese direkt ab Start)

Teilnahme Informationsaustausch
+ 1 Jahr
Verpflichtend für Besonders Wichtige

Start Nachweispflicht
+ 3 Jahre
(Betreiber kritischer Anlagen, andere auf Nachfrage)

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

KritisDG - physische Sicherheit

- Alle 4 Jahre: Risikoanalysen und -bewertungen!

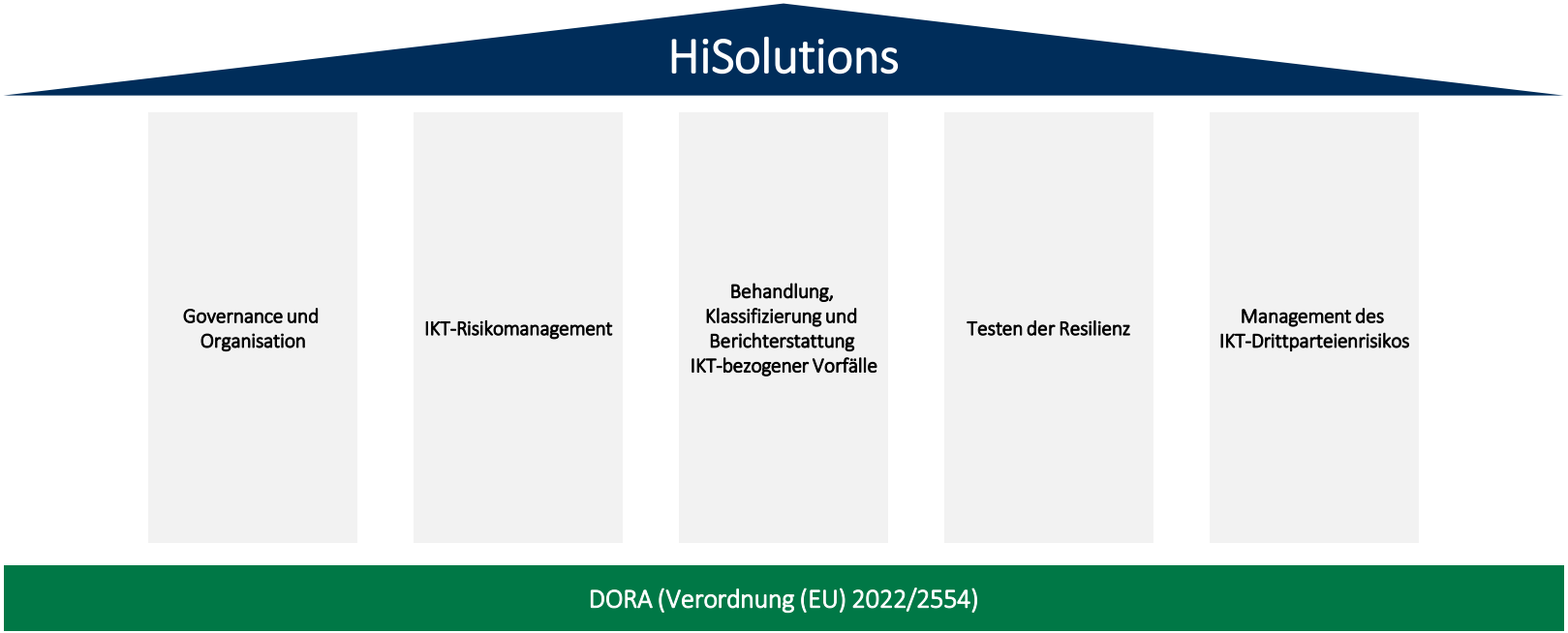
„Wirtschafsstabilität beeinträchtigenden, ***naturbedingten****,* ***klimatischen*** *und vom Menschen verursachten Risiken berücksichtigen, darunter solche* ***sektorübergreifender oder grenzüberschreitender Art****,* ***Unfälle****,* ***Naturkatastrophen****,* ***gesundheitliche Notlagen****, sowie* ***hybride Bedrohungen*** *oder andere* ***feindliche Bedrohungen****, einschließlich* ***terroristischer Straftaten****“ sowie „Wirtschafsstabilität beeinträchtigenden, Risiken berücksichtigen, die sich aus dem* ***Ausmaß der Abhängigkeiten anderer Sektoren*** *von der kritischen Dienstleistung, die von der kritischen Anlage –* ***auch in benachbarten Mitgliedstaaten und Drittstaaten*** *– erbracht wird“*

- Alle 2 Jahre: Resilienzplan nachweisen!

Die Aufgaben

Prävention	Physischer Schutz	Vorfalls- und Krisenmanagement
Verhindern von Sicherheitsvorfällen, unter gebührender Berücksichtigung von Katastrophenvorsorge und Maßnahmen zur Anpassung an den Klimawandel	Physischer Schutz von Räumlichkeiten und kritischen Infrastrukturen gewährleisten zum Beispiel durch Aufstellen von Zäunen und Sperren, Instrumenten und Verfahren für die Überwachung der Umgebung, Detektionsgeräten und Zugangskontrollen	Kapazitäten zur Reaktion, Abwehr und Folgeeinschränkung bei Vorfällen, unter gebührender Berücksichtigung der Umsetzung von Risiko- und Krisenmanagementverfahren und -protokollen und vorgegebener Abläufe im Alarmfall
Wiederanlauf	**Sicherheitsmanagement**	**Sensibilisierung von Personal**
Gewährleistung von Wiederherstellung, unter gebührender Berücksichtigung von Maßnahmen zur Aufrechterhaltung des Betriebs und der Ermittlung alternativer Lieferketten, um die Erbringung des wesentlichen Dienstes wiederaufzunehmen	Berücksichtigung von Maßnahmen wie Festlegung von Personalkategorien, Zugangsrechten zu Räumlichkeiten, kritischen Infrastrukturen und zu sensiblen Informationen und der Einführung von Verfahren für Zuverlässigkeitsüberprüfungen, Festlegung von Schulungsanforderungen und Qualifikationen	Personal für die unter den Maßnahmen unter gebührender Berücksichtigung von Schulungen, Informationsmaterial und Übungen zu sensibilisieren

DORA teilt sich in 5 Hauptthemen auf



IKT-Risikomanagementrahmen – Die IKT-Risikokontrollfunktion Artikel 6 DORA

Umsetzungs-verantwortung

Verantwortung

- Überwachung der Einhaltung des IKT-Risikomanagementrahmens
- Überwachung von IKT-Risiken (inkl. Drittparteien)
- Weiterentwicklung und kontinuierliche Verbesserung des IKT-Risikomanagementrahmens
- Schulung und Sensibilisierung der MA
- Für Transparenzverantwortung für Verstöße*
- Sicherstellung, für systematischen Umgang mit IKT-Risiken

2nd Line of Defense

Befugnisse & Kenntnisse

- Zur Festlegung und Durchsetzung des IKT-Risikomanagementrahmens
- Involvierung in alle Belange und Vorgänge mit Bezug zur digitalen Resilienz
- Budgetverantwortung für Risikobehandlungsmaßnahmen
- Vorspracherecht direkte Berichterstattung an Leitungsorgan
- Überwachung und Beanstandung IKT-Maßnahmen
- Unabhängigkeit von überwachten internen Einheiten
- Befugnis zur Beantragung von erf. Ressourcen
- Verständnis, Bewertung und Steuerung von IKT-Risiken

IKT-Risikomanagementrahmen
Aufgaben der IKT-Risikokontrollfunktion

IKT-Risikomanagement

- Unterstützung bei der Erarbeitung und Bewertung der DOR-Strategie
- Erstellung der IKT-Risikomanagementrichtlinie
- Steuerung & Koordination der IKT-Risikomanagementprozesse
- Festlegung von Methoden & Prozessen für IKT-Risikobewertung & Risikobehandlung
- Überprüfung & Initiierung von Verbesserungen zum IKT-Risikomanagementrahmen
- Bewertung der Auswirkungen von Veränderungen am IKT-Risikomanagementrahmen
- Bewertung von Maßnahmen zur Risikobehandlung der 1st Line of Defense
- Überwachung des IKT-Risikoprofils mit Bezug zum Gesamtrisikoprofil
- Überwachung des IKT-Risikoinventars und der Einhaltung des Risikoappetits
- Überwachung der IKT-Risiken in IKT-Projekten und beim Drittbezug von IKT-Dienstleistungen
- Beurteilung von Verstößen gegen den Risikoappetit
- Monitoring technologischer Entwicklungen mit Relevanz für digitale Resilienz
- Überwachung von akzeptierten IKT-Restrisiken und Ausnahmeregelungen

IKT-Risikomanagementrahmen

Aufgaben der IKT-Risikokontrollfunktion

IKT-Sicherheitsmanagement

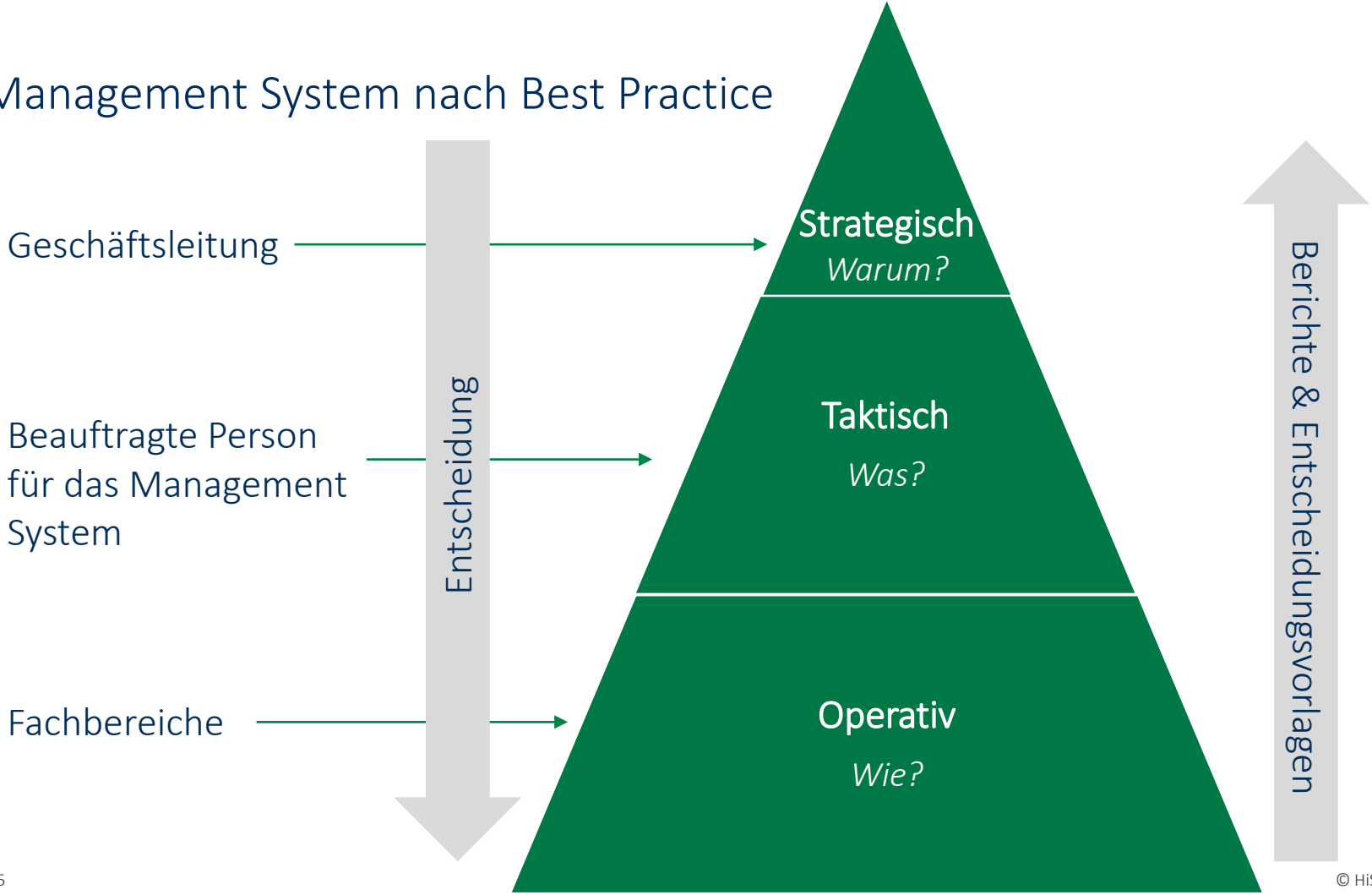
- Erstellung der Informations-Sicherheitsrichtlinie sowie Definition von 2nd LoD-Vorgaben dazu
- Überwachung von Implementierungsaktivitäten zu IKT-Sicherheitsrichtlinien
- Beanstandung von Verstößen gegen IKT-Sicherheitsrichtlinien
- Koordination der Erstellung von IKT-Sicherheitsrichtlinien und -verfahren
- Überwachung der Einhaltung von IKT-Sicherheitsrichtlinien
- Überwachung der Implementierung von IKT-Sicherheitsmaßnahmen
- Beanstandung von Mängeln der Implementierung von IKT-Sicherheitsmaßnahmen
- Steuerung & Koordination der Informationssicherheitsprozesse
- Überwachung der Informationssicherheit in IKT-Projekten
- Überwachung & Auswertung von IKT-Vorfällen
- Überwachung der Informationssicherheit bei der IKT-Beschaffung
- Unterstützung und Beratung bei der Erstellung von IKT-BCM-Plänen
- Unterstützung bei der Erstellung von Response- & Recovery-Plänen

IKT-Risikomanagementrahmen
Aufgaben der IKT-Risikokontrollfunktion

Operative Aufgaben und Unterstützung

- Reporting & Beratung des Leitungsgremiums zu Fragen der digitalen Resilienz
- Beantwortung von Anfragen zur digitalen Resilienz und Sicherheit durch Dritte
- Bereitstellung von Informationen, Analysen & Meinungen zu IKT-Risiken
- Beratung der Fachbereiche zu Fragestellungen im Bereich der IKT-Risiken
- Plausibilisierung der Kritikalitätsbewertung von Assets
- Überwachung der Implementierung von IKT-Sicherheitsmaßnahmen
- Monitoring technologischer Entwicklungen mit Relevanz für die digitale Resilienz
- Überwachung der Informationssicherheit in der IKT-Beschaffung
- Plausibilisierung der Einwertung von kritischen Bereichen und wichtigen Funktionen

Management System nach Best Practice

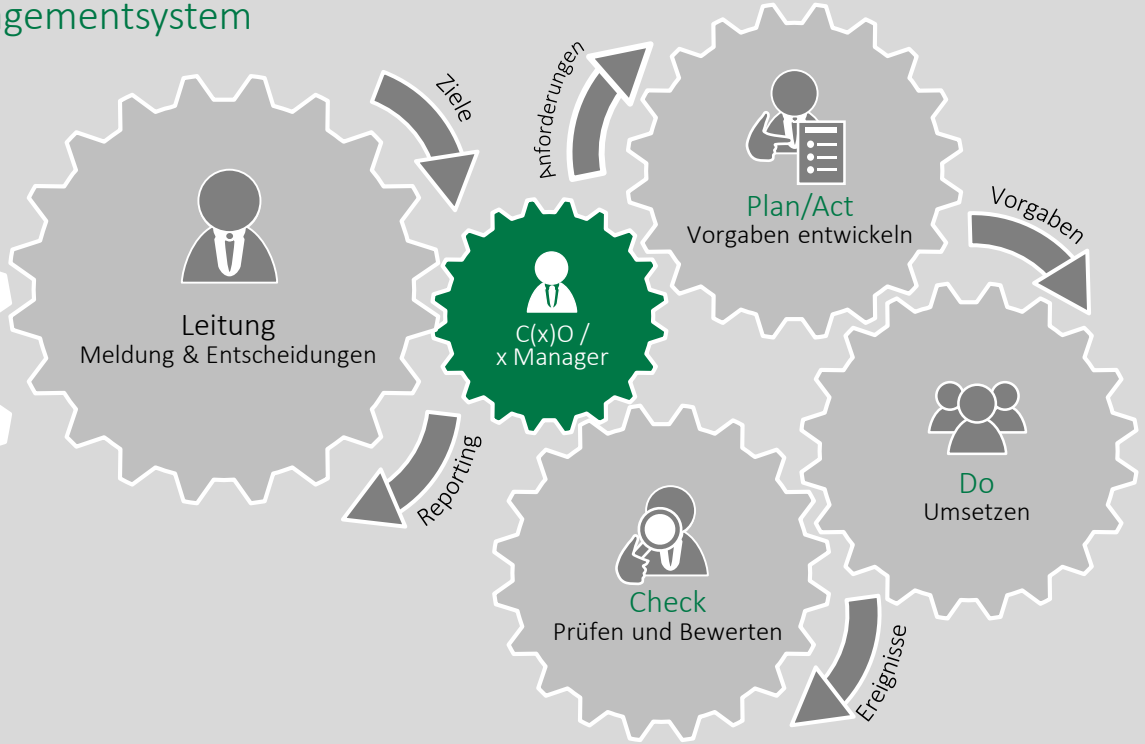


Allgemeiner Aufbau Managementsystem

Stakeholder

- Kunden
- Staat
- Aufsichtsorgane
- Mitarbeitende
- Leitung
- Partner und Partnerinnen
- Lieferanten
- Märkte

Managementsystem

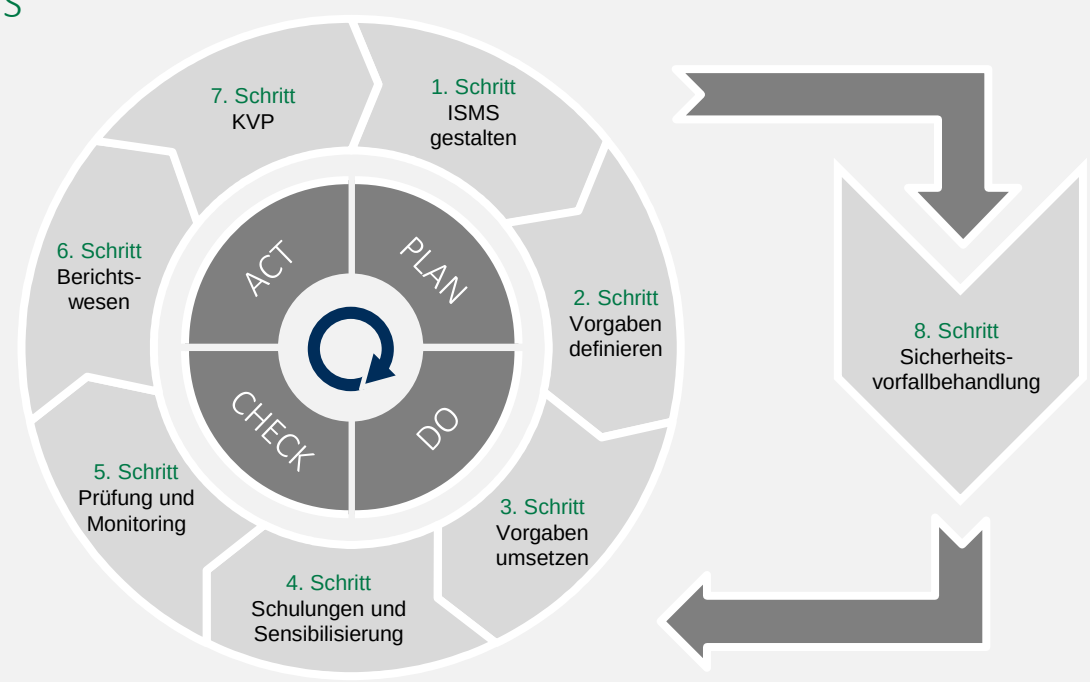


Klassisches Informationssicherheitsmanagement (ISMS)

ISMS-Anforderungen

- Gesetzliche Vorgaben
- Externe Vorgaben
- Konzernanforderungen
- Unternehmensziele
- Interne Anforderungen

ISMS



Strukturierte Vorgehensweise der Implementierung

Neuer RefE NIS-2 von Mai 2025

- Systeme zur Angriffserkennung nur für die KRITIS-Anlagen, nicht generell
- Einrichtungen der Bundesverwaltung müssen nach 3 statt 5 Jahren Erfüllung der Anforderungen nachweisen
- Einrichtungen der Bundesverwaltung müssen BSI IT-Grundschutz und Mindeststandards erfüllen
- Überarbeitung BSI IT-Grundschutz bis 1.1.2026
- BSI-Kritisverordnung gestrichen, heißt jetzt "Verordnung zur Bestimmung kritischer Anlagen nach dem BSI-Gesetz"

Neuer RefE NIS-2 von Mai 2025

- Neuer KRITIS Sektor "Sektor Sozialversicherungsträger sowie Grundsicherung für Arbeitssuchende"
- Neu: "Digitaler Energiedienst"
- Detaillierte Haushaltsausgaben werden für alle Ministerien bis 2029 aufgeführt
- Klärung von DNS-Diensteanbieter, MSSP und MSP
- KRITIS-Dachgesetz komplett entfernt, Harmonisierung erfolgt offenbar doch nicht
- Cyberhygiene gestrichen, heißt jetzt "Schulungen und Sensibilisierungsmaßnahmen"

HISOLUTIONS

Schloßstraße 1 | 12163 Berlin

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

www.hisolutions.com