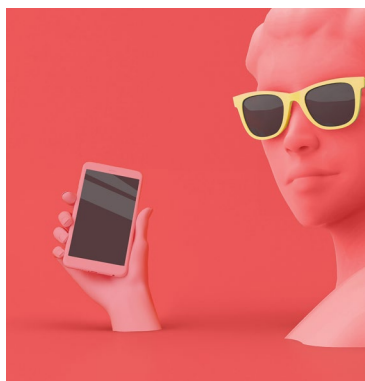


ENABLING
PEOPLE
IMPROVING
BUSINESS



ISO 27001, NIS2 UND DORA IM VERGLEICH

**Synergien, Lücken und
Handlungsempfehlungen**

Anforderungen verstehen,
Unterschiede erkennen,
Lücken schließen

EXECUTIVE SUMMARY



Viele Unternehmen haben den Grundstein für NIS2 und DORA bereits gelegt – insbesondere jene, die nach ISO/IEC 27001 zertifiziert sind. Die gute Nachricht: Die drei Regelwerke weisen zahlreiche Überschneidungen auf – insbesondere in den Bereichen Risikomanagement, technische und organisatorische Maßnahmen sowie Cyber-Awareness.

Doch trotz inhaltlicher Nähe gibt es wesentliche Unterschiede, insbesondere im Hinblick auf Verbindlichkeit, Meldepflichten und regulatorische Kontrolle. Dieses Whitepaper zeigt auf, wo Synergien liegen, wo Lücken klaffen und wie Unternehmen gezielt handeln können, um NIS2- und DORA-konform zu werden.

INHALT

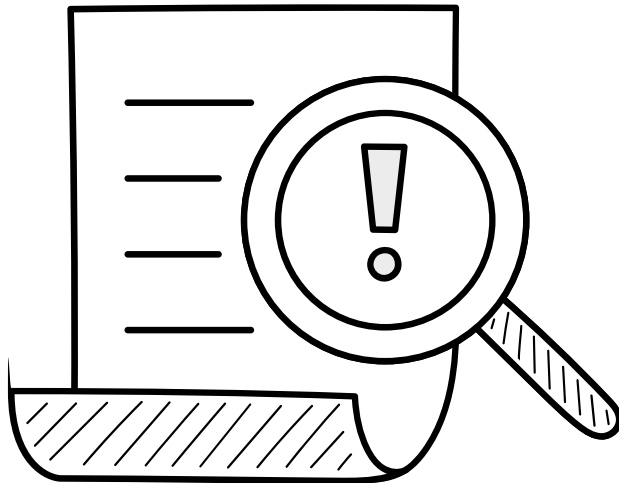


Grundlagen: Wofür stehen ISO/IEC 27001, NIS2 und DORA?	// 05
Gemeinsamkeiten & Synergien von ISO/IEC 27001, NIS2 & DORA	// 09
Risikomanagement, Technische und organisatorische Maßnahmen, Cyber-Awareness & Schulungen und Lieferkettenmanagement	
Unterschiede & zusätzliche Anforderungen von NIS2/DORA gegenüber ISO 27001	// 12
Verpflichtender Charakter, Meldepflichten, Sanktionen & Haftung, Lieferkettensicherheit und Behördliche Aufsicht	
Fazit – der Weg ist kürzer als gedacht	// 23
Unsere Empfehlung – für ISO-zertifizierte Unternehmen & Unternehmen ohne ISO 27001	// 25

GRUNDLAGEN



WOFÜR STEHEN ISO/IEC 27001, NIS2 UND DORA?



ISO/IEC 27001

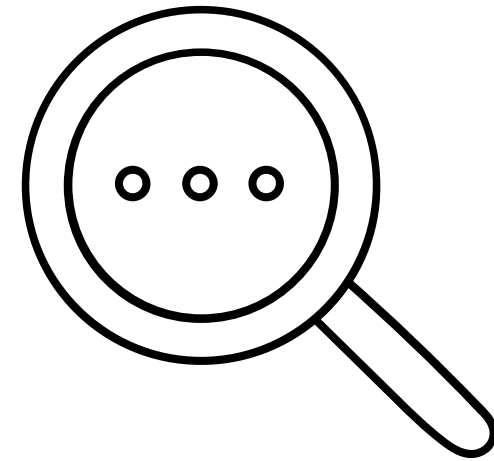
→ Die ISO/IEC 27001 ist ein international anerkannter Standard für den Aufbau, Betrieb und die kontinuierliche Verbesserung eines Informationssicherheitsmanagementsystems (ISMS).

Zentrale Elemente sind:

- Systematisches Risikomanagement
- Sicherheitsrichtlinien und Maßnahmen
- Freiwillige Zertifizierung als Nachweis für gelebte IT-Sicherheit

Sie ist weltweit etabliert, insbesondere in stark regulierten Branchen (z. B. Automotive, Finanzwesen, Gesundheit).





NIS2 (EU-RICHTLINIE FÜR NETZ- UND INFORMATIONSSICHERHEIT)

→ Die NIS 2-Richtlinie ist eine verbindliche EU-weite Richtlinie, die Unternehmen aus kritischen und wichtigen Sektoren verpflichtet, konkrete Maßnahmen zur Cyberresilienz, Lieferkettensicherheit und zum Vorfallmanagement zu implementieren. Aktuell wird diese Richtlinie in nationales Recht übertragen.

Besonderheiten:

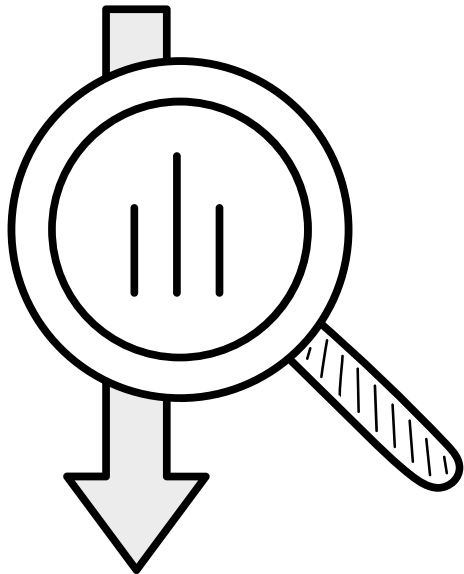
- Fokus auf digitale Widerstandsfähigkeit
- Strenge Meldepflichten
- Starke Aufsichts- und Sanktionsmechanismen

Wichtig:

Die gesetzliche Verabschiedung in Deutschland ist zwar verspätet, aber die EU-weite Anwendbarkeit der Richtlinie bleibt bestehen. (Stand: April 2025 – Gesetzesentwurf (NIS2UmsuCG))

In der Praxis empfiehlt es sich daher für Unternehmen aus den betroffenen Sektoren, bereits jetzt so zu handeln, als sei NIS2 in Kraft. Eine frühzeitige Orientierung an den EU-Vorgaben ist ratsam, da rückwirkende Anforderungen und Prüfpflichten nicht ausgeschlossen werden können.





DORA (DIGITAL OPERATIONAL RESILIENCE ACT)

→ DORA ist eine EU-Verordnung und gilt somit unmittelbar für die betroffenen Unternehmen. Sie dient zur digitalen operationellen Resilienz im Finanzsektor.

Kerninhalte:

- Cybersicherheits- und Resilienzanforderungen für Banken, Versicherungen, Zahlungsdienstleister etc.
- Umfassende Anforderungen an ICT-Risikomanagement, Drittanbieter-Kontrolle und Incident Reporting
- Gilt verbindlich ab Januar 2025

GEMEINSAMKEITEN & SYNERGIEN

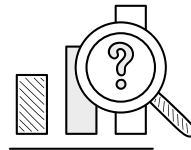


GEMEINSAMKEITEN & SYNERGIEN VON ISO/IEC 27001, NIS2 & DORA



Viele Anforderungen überschneiden sich, was es Unternehmen ermöglicht, bereits bestehende Sicherheitskonzepte weiterzuverwenden und gezielt zu erweitern.

Im Detail handelt es sich dabei um folgende Punkte:

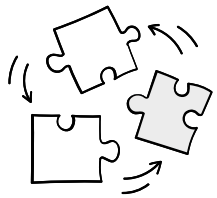


RISIKOMANAGEMENT:

Alle drei Regelwerke fordern ein umfassendes, dokumentiertes Risikomanagement. Während in der ISO 27001 auf die Risikomanagement-Leitlinie aus ISO 31000 verwiesen wird, werden in DORA und bei NIS2 keine spezifischen Methoden vorgegeben, Meldepflichten hängen aber dennoch unmittelbar an der Risikobewertung.

Wer ein ISMS nach ISO/IEC 27001 betreibt, erfüllt hier bereits wesentliche Vorgaben – inklusive Risikobewertung, -behandlung und -überwachung.

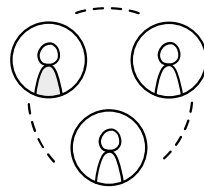




TOMS - TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN:

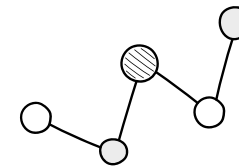
Zentrale TOMs nach ISO 27001 wie:

- Zugriffskontrollen
 - Schwachstellenmanagement
 - Backup-Strategien
 - Protokollierung & Monitoring
- ...bilden auch die Basisanforderungen in NIS2 und DORA.



CYBER-AWARENESS & SCHULUNGEN:

Regelmäßige Awareness-Maßnahmen für Mitarbeitende und Führungskräfte sind in allen drei Regelwerken vorgesehen. Bei NIS 2 werden im Gegensatz zur ISO 27001 diese Pflichten für Führungskräfte explizit verpflichtet.



LIEFERKETTEN-MANAGEMENT:

Während ISO 27001 Lieferkettenrisiken bereits adressiert, fordern NIS2 und DORA explizit **Verantwortlichkeit für die Cybersicherheit Dritter** – inklusive Monitoring, vertraglicher Absicherung und Nachweispflichten.

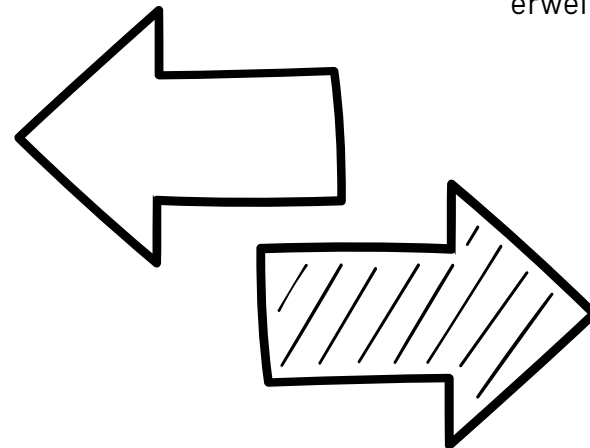
UNTERSCHIEDE & ANFORDERUNGEN



UNTERSCHIEDE & ZUSÄTZLICHE ANFORDERUNGEN VON NIS2/DORA GEGENÜBER ISO 27001



Trotz der vielen Parallelen gibt es entscheidende Unterschiede, die Unternehmen berücksichtigen müssen:



VERPFLICHTENDER CHARAKTER

ISO/IEC 27001:

freiwillig, aber marktgetrieben (oftmals vorausgesetzt als Bedingung für Geschäftsbeziehungen z.B. im Bereich Automotive oder im Finanzwesen)

NIS2 & DORA:

gesetzlich vorgeschrieben für betroffene Sektoren – inklusive behördlicher Kontrolle und Sanktionen

Im Gegensatz zu seinem Vorgänger NIS ist die NIS 2-Verordnung deutlich strenger, konkreter und umfasst einen erweiterten Anwendungsbereich.





Der Anwendungsbereich erstreckt sich über Einrichtungen, die ihre Dienste in der EU erbringen oder ihre Tätigkeit dort ausüben.

Neben einer Erweiterung der betroffenen Sektoren, spielt nun auch die Größe der Einrichtungen eine Rolle.

1

SEKTORENZUGEHÖRIGKEIT

Das Unternehmen muss in einem der in der Richtlinie definierten Sektoren oder Teilsektoren tätig sein:

- Kritische Sektoren (z. B. Energie, Gesundheit, Verkehr, Trinkwasser)
- Wichtige Sektoren (z. B. digitale Dienste, Lebensmittel, Chemie, Postdienste)
- Öffentliche Verwaltungen bestimmter Größenordnung (insbesondere zentrale staatliche Stellen auf nationaler oder regionaler Ebene)

2

GRÖSSENKRITERIUM

Die NIS2-Richtlinie gilt in der Regel für Unternehmen, die:

- mindestens 50 Beschäftigte haben oder
- einen Jahresumsatz bzw. Jahresbilanzsumme von über 10 Mio. Euro

3

SONDERREGELUNGEN (UNABHÄNGIG VON DER GRÖSSE)

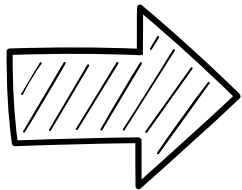
Auch kleinere Unternehmen können betroffen sein, wenn:

- Sie eine wesentliche Rolle für Gesellschaft oder Wirtschaft spielen (z. B. Monopolstellung)
- Sie alleiniger Anbieter eines kritischen Dienstes in einer Region oder einem Land sind
- Ein hohes Sicherheitsrisiko durch Angriffe oder Ausfälle vorliegt

(>> Ob ein Unternehmen in die Sonderregelung fällt, ist unter Artikel 2(2) in der NIS2-Richtlinie geregelt)

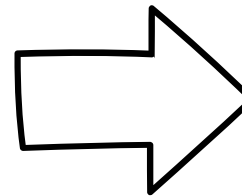
18 SEKTOREN

→ Insgesamt fallen in die NIS2-Richtlinie 18 Sektoren



KRITISCHE SEKTOREN:

- Energie
- Transport
- Gesundheit
- Öffentliche Verwaltung
- Abwasser
- Digitale Infrastruktur
- Verwaltung von IKT-Diensten
- Bankwesen
- Finanzmärkte
- Trinkwasser
- Weltraum



WICHTIGE SEKTOREN:

- Abfallwirtschaft
- Digitale Dienste
- Lebensmittel
- Chemie
- Postdienste
- Industrie
- Forschung

MELDEPFLICHTEN



Die **ISO 27001** fordert kein gesetzlich vorgeschriebenes Reporting, aber ein strukturiertes Incident Management.

NIS2 & DORA sehen eine strenge Meldepflicht erheblicher Sicherheitsvorfälle an Behörden vor.

DER MELDEPROZESS NACH DORA FÜR DAS FINANZWESEN IST EIN DREISTUFIGER PROZESS:

Stufe	Frist	Inhalt
1. Frühwarnung	innerhalb von 4 Stunden nach Entdeckung	Erste Einschätzung des Vorfalls, auch wenn noch keine vollständigen Infos vorliegen.
2. Erstmeldung	innerhalb von 24 Stunden	Beschreibung des Vorfalls, vermutete Ursache, betroffene Systeme & erste Maßnahmen.
3. Abschlussbericht	innerhalb von 1 Monat nach Erstmeldung	Detaillierte Analyse, Lessons Learned, Maßnahmen zur Verhinderung zukünftiger Vorfälle.

Empfänger sind Nationale Aufsichtsbehörden, also z.B. die BaFin und ggf. EZB bzw. EBA





DER MELDEPROZESS NACH NIS 2 UMFASST 4 MELDESTUFEN:

Stufe	Frist	Inhalt
1. Frühwarnung ("early warning")	innerhalb von 4 Stunden nach Entdeckung	Erste Einschätzung des Vorfalls, auch wenn noch keine vollständigen Infos vorliegen.
2. Incident Notification	innerhalb von 24 Stunden	Beschreibung des Vorfalls, vermutete Ursache, betroffene Systeme & erste Maßnahmen.
3. Interimsbericht (optional)	innerhalb von 1 Monat nach Erstmeldung	Detaillierte Analyse, Lessons Learned, Maßnahmen zur Verhinderung zukünftiger Vorfälle.
4. Abschlussbericht	innerhalb eines Monats	Vollständige Analyse, konkrete Auswirkungen, Lessons Learned, ggf. Meldepflicht an betroffene Kunden.

Empfänger sind nationale Cybersicherheitsbehörden, z.B. in Deutschland das BSI.

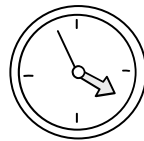


WAS NIS 2 UND DORA GEMEINSAM HABEN SIND:



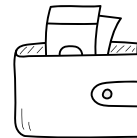
FRÜHWARNPRINZIP

Schnelles Handeln zählt
mehr als Vollständigkeit



STUFENBASIERTER ABLAUF

Unternehmen haben Zeit,
ihre Meldung zu verfeinern



HOHE BUSSGELDER

Bei Nichterfüllung der
Meldepflichten (bis zu
10 Mio. € oder mehr)



DOKUMENTATIONSPFLICHT

Alle Schritte müssen
intern nachvollziehbar
dokumentiert sein

SANKTIONEN & HAFTUNG

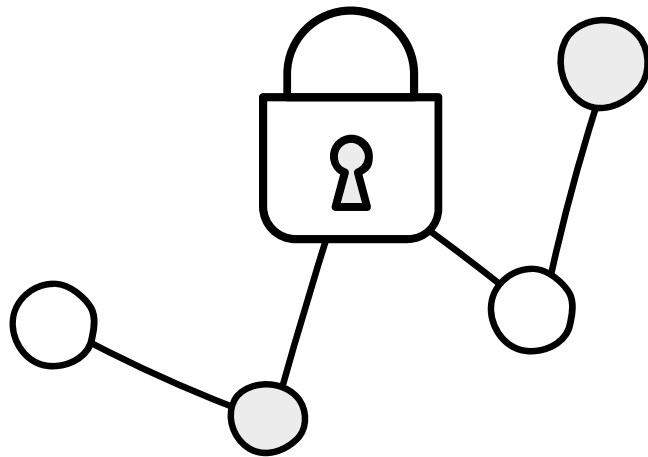
→ **Verstöße gegen NIS2 oder DORA** können Bußgelder bis zu **10 Mio. € oder 2 % des weltweiten Jahresumsatzes** nach sich ziehen. In Einzelfällen droht persönliche Haftung von Geschäftsführenden.

NIS 2 verlangt explizit, dass die **Geschäftsführung** in die Cybersicherheitsstrategie des Unternehmens eingebunden ist. Dabei sind sie zudem verpflichtet regelmäßig Fortbildungen zu diesem Thema zu absolvieren.

Bei **DORA** besteht für die **Geschäftsführung** die Pflicht zur Überwachung des IKT-Risikomanagements.

ACHTUNG: Die **persönliche Haftung**
der Geschäftsführung ist also
nicht nur eine theoretische,
sondern auch eine **strukturell**
verankerte Komponente.

LIEFERKETTENSICHERHEIT

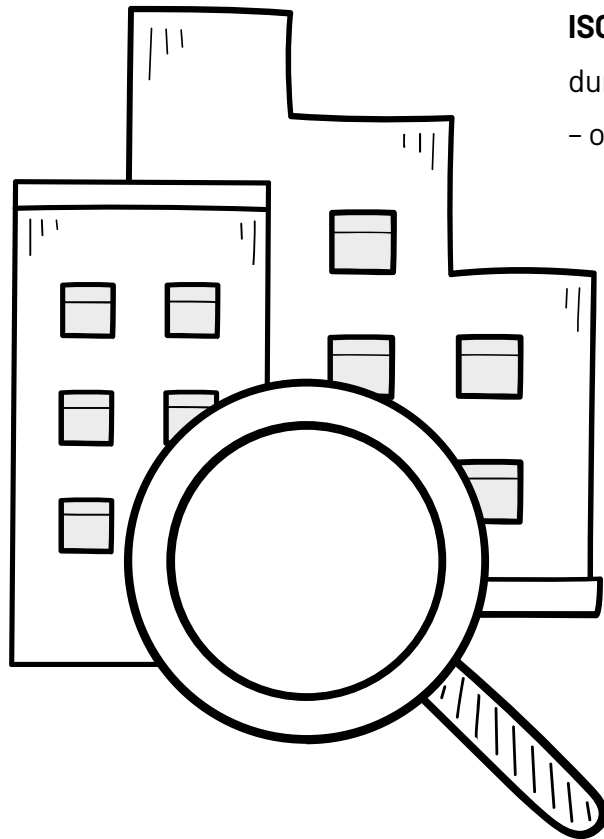


ISO 27001: Berücksichtigt Lieferketten im Risikomanagement, jedoch ohne regulatorische Durchgriffsrechte. Eine Überprüfung von Lieferanten und Dritten wird als ein optionales Kontrollfeld betrachtet.

NIS2/DORA: Unternehmen müssen Sicherheitsanforderungen **an Dritte übertragen, überwachen und nachweisen**

Dora sieht dabei explizit regelmäßige Risikoanalysen für IKT-Dienstleister vor. Dabei kann es auch zu Vertragskündigen kommen, wenn grobe Mängel vorliegen.

BEHÖRDLICHE AUFSICHT



ISO 27001: Externe Audits erfolgen durch private Zertifizierungsstellen – ohne staatliche Eingriffe

NIS2/DORA: Im Rahmen von NIS2 und DORA erhalten Behörden wie das BSI umfassende Prüf-, Anordnungs- und Durchsetzungsbe-fugnisse. In der Praxis äußert sich das unter anderem in Form von Vor-Ort-Kontrollen, Penetrationstests durch externe Dienstleister oder gezielten Audits durch europäische Aufsichtsbehörden (ESAs). Die damit verbundene Aufsicht reicht deutlich über das hinaus, was viele Unternehmen bislang aus ISO 27001-Audits gewohnt sind.

FAZIT



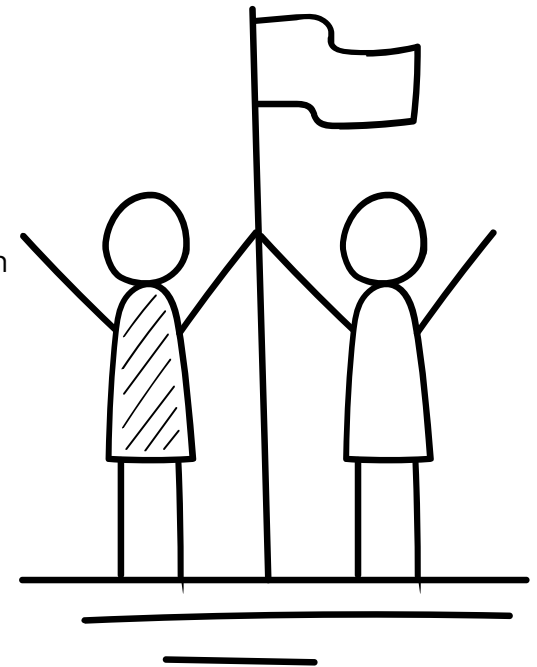
VON DER ISO-ZERTIFIZIERUNG ZUR NIS2-/DORA-COMPLIANCE - DER WEG IST KÜRZER ALS GEDACHT



Unternehmen mit einem bestehenden ISMS nach ISO 27001 haben einen klaren Vorteil: **Strukturen, Prozesse und Maßnahmen sind bereits vorhanden** – und bilden die Grundlage für eine zielgerichtete Umsetzung von NIS2 und DORA.

Doch: **Ergänzungen sind zwingend erforderlich**, insbesondere in den Bereichen strukturiertes Vorfallmanagement, frühzeitige Meldeprozesse, erweiterte Lieferkettentransparenz sowie klar dokumentierte und prüfbare Nachweispflichten gegenüber Behörden.

Auch können, je nach Branche, spezifische Tests auf Unternehmen zukommen. Das könnte im Fall von DORA sogenannte Threat-Led Penetration Testings (TLPT) umfassen. Dabei geht es um Tests, welche echte Bedrohungsszenarien abbilden sollen und die Resilienz gegenüber komplexen Cyberangriffen überprüfen. Die in NIS 2 geforderten Governance-Anforderungen an Führungskräfte können ebenfalls bestehende Lücken sein, die strukturelle Anpassungen mit sich bringen und bedacht werden müssen.



UNSERE EMPFEHLUNG



FÜR ISO-ZERTIFIZIERTE UNTERNEHMEN



Nutzen Sie Ihre bestehenden Strukturen als Fundament – und schließen Sie gezielt die Lücken.

Wir unterstützen Sie bei der:

- Gap-Analyse zwischen ISO 27001, NIS2 & DORA
- Etablierung gesetzeskonformer Meldeprozesse
- Implementierung von Kontroll- und Dokumentationspflichten
- Einführung von Zero-Trust-Architektur

FÜR UNTERNEHMEN OHNE ISO 27001



Ein ISMS nach ISO/IEC 27001 ist nicht nur ein bewährter Standard – sondern ein idealer Einstiegspunkt zur Erfüllung regulatorischer Anforderungen. Die klar definierten Maßnahmen erleichtern die Umsetzung erheblich – und bieten langfristige Vorteile durch Struktur, Transparenz und Reputation.

WEITERE INFOS

Sie haben Fragen oder wollen unverbindlich beraten werden? Wir beraten Sie gerne.

IHR ANSPRECHPARTNER:

Heiko Wessels | Senior Sales Manager
heiko@provectus.de
+49 (0) 89 710 409 20



Kostenloses Beratungsgespräch

