RISIKOMANAGEMENT · gehört auf · C-LEVEL

Das Ende der *3-Jahres-Strategieplanung.*

Die Welt verändert sich schneller als jeder Strategieplan. Es gibt ein Führungsinstrument, das damit Schritt hält – und das die EU bereits verpflichtend fordert.

ISO

31000

Internationaler Standard für Risikomanagement

Nicht Bürokratie.
Ein Denkrahmen für Führung.

01 **Prinzipien**

Risiko und Chance als Wertschöpfung

Risiko als strategische Variable begreifen – nicht als Bedrohung, die es zu vermeiden gilt.

02 **Rahmenwerk**

Verankerung auf Führungsebene

Klare Verantwortlichkeiten, Ressourcen und Kommunikation auf C-Level.

03 **Prozess**

Kontinuierlicher Zyklus

Identifizieren, Bewerten, Behandeln, Überwachen, Kommunizieren – dauerhaft.

DER ISO 31000 PROZESS

5 Schritte. Kontinuierlich. Nicht einmalig.

Der Prozess ist kein Projekt – er ist eine Führungsroutine.

01

Kontext bestimmen

Interne & externe Faktoren, Stakeholder und Ziele präzise definieren

02

Risiken identifizieren

Was kann passieren? Wo, warum und mit welchen Folgen?

03

Risiken bewerten

Eintrittswahrscheinlichkeit × Auswirkung = Priorisierung

04

Risiken behandeln

Vermeiden, reduzieren, transferieren oder bewusst akzeptieren

05 **Überwachen & Kommunizieren** — Kontinuierliches Monitoring & Reporting auf Führungsebene

EU-REGULIERUNG

5 Gesetze.

1 gemeinsamer Kern.

NIS2

Cyber-Risikomanagement als Pflicht. Persönliche GF-Haftung. Ab 50 Mitarbeitenden oder 10 Mio. € Umsatz.

DORA

IKT-Risikomanagement im Finanzsektor. Bußgeld bis zu 2 % des weltweiten Jahresumsatzes.

AI Act

Risikoklassifizierung für KI-Systeme verpflichtend. Sanktionen bis 35 Mio. € oder 7 % Umsatz.

CRA

Cyber Resilience Act: Security by Design – Risikomanagement über den gesamten Produktlebenszyklus.

DSGVO

Datenschutz-Folgenabschätzung (DSFA) als formalisiertes Risikoinstrument. Artikel 32 DSGVO.

Quelle: NIS2UmsuCG, DORA, EU AI Act, CRA, DSGVO

FÜHRUNGSINSTRUMENT IM VERGLEICH

Warum Risikomanagement Controlling & Strategiepläne schlägt.

Gestern

— 3-Jahres-Plan: starr, oft nach 6 Monaten überholt

— Controlling: blickt in den Rückspiegel

— Reaktiv: Schaden wird erst nach Eintritt sichtbar

— Entscheidungen auf Basis von Vergangenheitsdaten

— Risiko als Störfaktor – nicht als Variable

Heute: ISO 31000

✓ Rollierend & dynamisch – passt sich der Realität an

✓ Zukunftsgerichtet: Szenarien & Frühwarnsignale

✓ Proaktiv: Risiken behandelt, bevor sie Schaden anrichten

✓ Echtzeit-Entscheidungen mit Risikoklarheit

✓ Risiko als strategische Steuerungsgröße

C-LEVEL VERANTWORTUNG

Risikomanagement ist Chefsache. Nicht IT-Sache.

Persönliche Haftung

NIS2 & DORA verankern die Verantwortung explizit beim Geschäftsführer. Keine Delegation möglich – mit echten Konsequenzen.

Strategische Entscheidungsgrundlage

Jede Investition, jede Partnerschaft, jedes Produkt – mit Risikoklarheit entscheiden statt mit Bauchgefühl.

Messbarer Wettbewerbsvorteil

Kunden, Partner und Investoren bevorzugen Unternehmen mit belastbarem, nachweisbarem Risikomanagement.

Resilienz in Zeiten des Wandels

KI-Superzyklus, Cyberbedrohungen, Regulierungswellen – nur wer Risiken kennt, steuert souverän durch Veränderung.

FAZIT

Risikomanagement ist keine Last.
Es ist Ihre Lizenz zum Wachsen.

Wer Risikomanagement als strategisches Führungsinstrument verankert, erfüllt gleichzeitig NIS2, DORA, AI Act, CRA und DSGVO – und entscheidet schneller, sicherer und souveräner als der Wettbewerb.

Haben Sie Risikomanagement bereits auf C-Level verankert – oder kämpfen Sie noch mit Einzelmaßnahmen und Jahresplänen?

Wir begleiten Unternehmen dabei, Risikomanagement als das zu etablieren, was es wirklich ist: das operative Rückgrat moderner Führung. Lassen Sie uns sprechen.

#Risikomanagement #ISO31000 #NIS2 #DORA #CyberSecurity #Compliance #CLevel #AIAct #Mittelstand