
MOORE Deutschland
Herzlich willkommen zu Tag 2
der Moore Deutschland
Jahrestagung 2026

MOORE Deutschland

Lösungsorientiert denken und handeln – Das Unmögliche als Grenzerfahrung

Jost Kobusch


MOORE Deutschland
Kaffeepause
mit Führungen durch
die Ausstellung

MOORE Deutschland

Im Kreuzfeuer – Wie globale Spannungen die Lieferketten verändern

Markus Bitzer

MOORE Deutschland

26.225

Störungsereignisse in globalen Lieferketten allein im Jahr 2025.

72 am Tag. Alle 20 Minuten eine.

Quelle Resilinc EventWatch, Jahresbericht Illumination 2025

Was da alles hineinfällt

Diese Störungen wirken nicht nacheinander, sondern gleichzeitig auf die Lieferkette.

112

laufende bewaffnete Konflikte weltweit, davon 34 internationale
(Geneva Academy, Nov. 2025)

71.871

aktive Sanktionsziele weltweit aus 93 Sanktionslisten
(OpenSanctions, Sept. 2026)

1.127

neue handelspolitische Maßnahmen in einem Jahr, Höchststand seit Beginn der Erhebung 2009 (WTO)

19,7 %

aller Weltimporte laufen inzwischen gegen Einfuhrbeschränkungen (WTO, Okt. 2025)

358

Naturkatastrophen im Jahr 2025 mit 224 Mrd. US-Dollar Gesamtschaden
(EM-DAT, Munich Re)

4 von 7

kritischen **Seewegen** der Welt sind 2026 **gestört**, darunter Hormus, Suez und Bab el-Mandeb

Eine Welt im Umbruch

Die alten Gewissheiten zerfallen

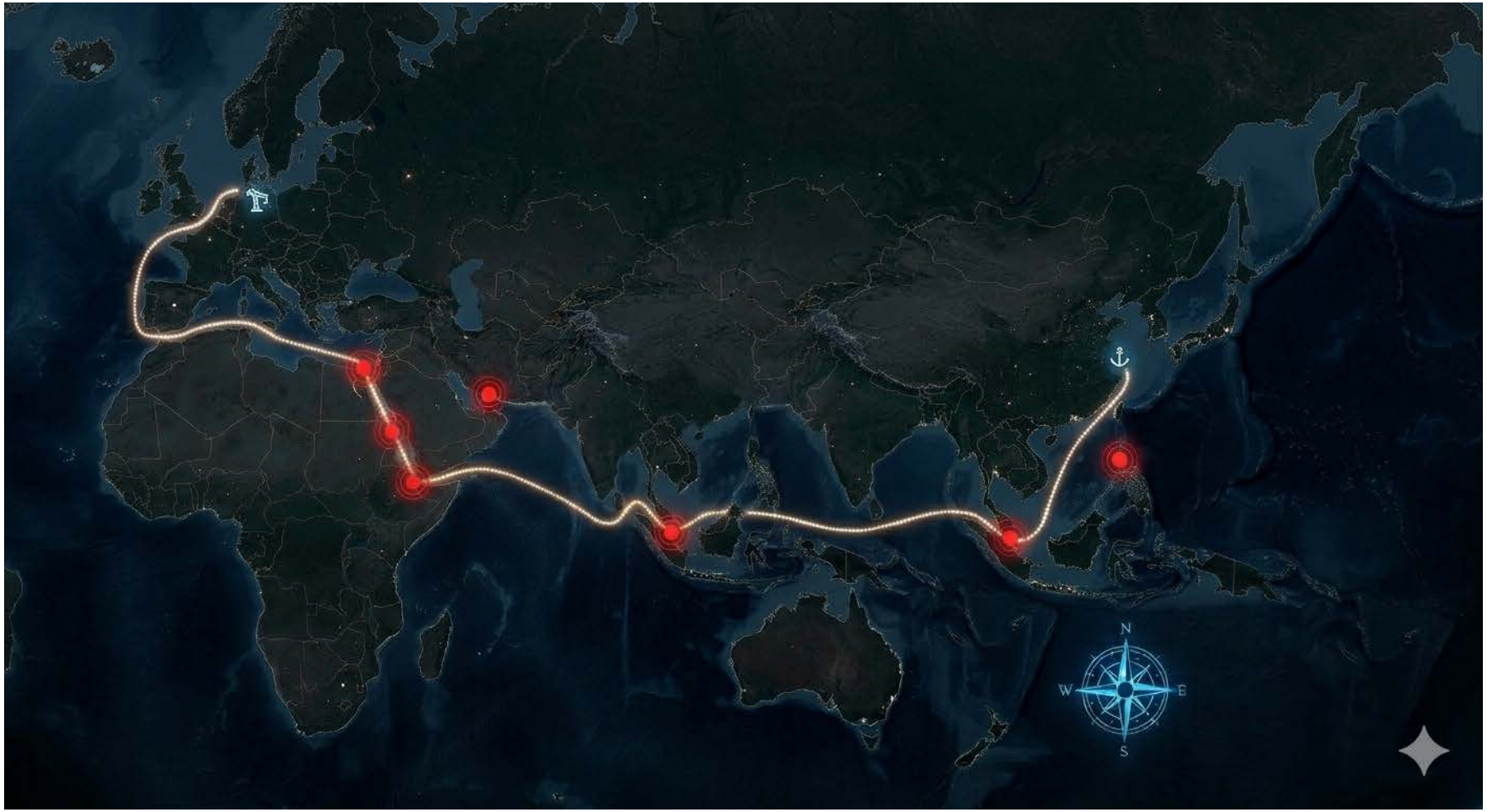
- Jahrzehntelang lief der Welthandel mit einer stillen Selbstverständlichkeit.
- Die Fundamente, auf denen moderne Lieferketten gebaut wurden, werden nun gleichzeitig auf die Probe gestellt.
- Was wir erleben, ist kein vorbeiziehendes Unwetter. Es ist das neue Klima.

Das Fundament bricht

Frieden, Freihandel und anerkannte Regeln stehen erstmals gleichzeitig unter Druck.

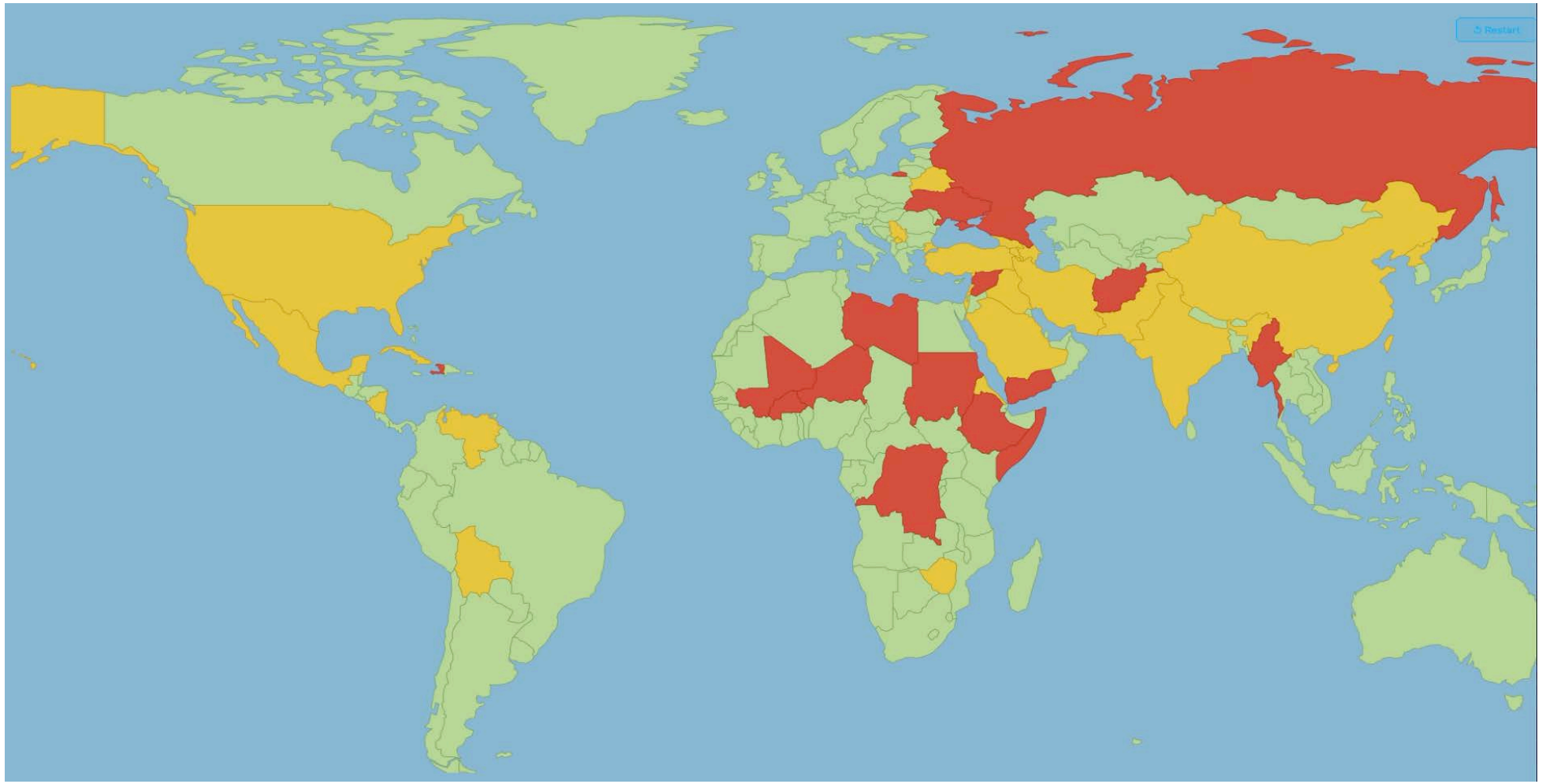
Der globale Hindernislauf

Die Reise einer einzigen Sendung nach Europa.



Der perfekte Sturm

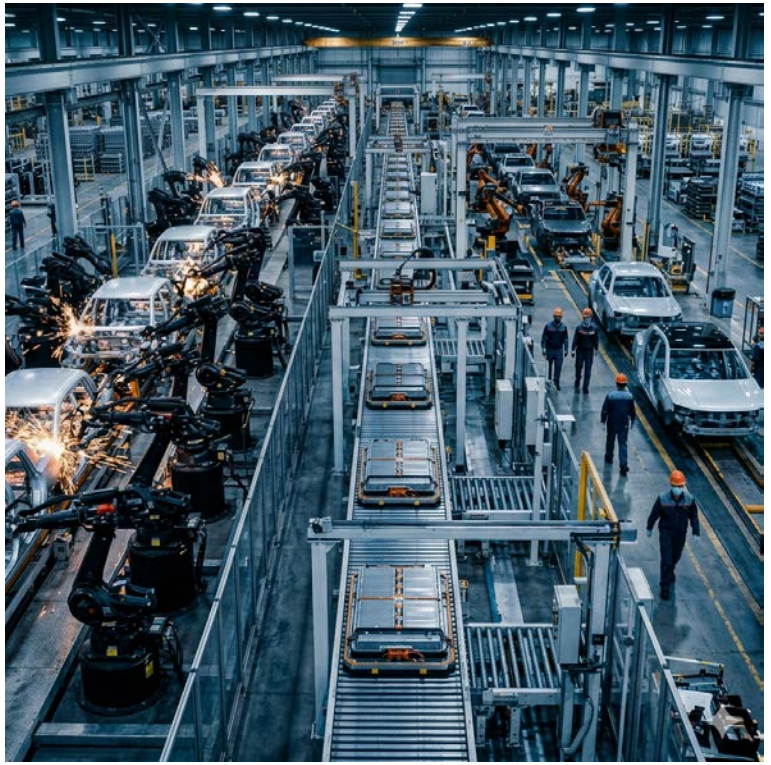
Alles zur gleichen Zeit!



Industrie und Automotive

Vier Wochen Produktionsstillstand nach einem Cyberangriff

- **Jaguar Land Rover** stand im September 2025 nach einem Cyberangriff vier Wochen still.
- Der Schaden für die britische Wirtschaft wird auf 1,9 Milliarden Pfund geschätzt.
- **Bei Nexperia** führte ein Streit zweier Staaten im Oktober 2025 zur Spaltung des Unternehmens.
- **Volkswagen** terminierte Stillstände, weil Transistoren für wenige Cent fehlten.
- Bei diesen Bauteilen hält ein einzelner Hersteller rund 40 Prozent des Weltmarkts.



Wer kennt den Lieferanten des Lieferanten?

Energie

Schiffsanker kappt Stromverbindung für sechs Monate

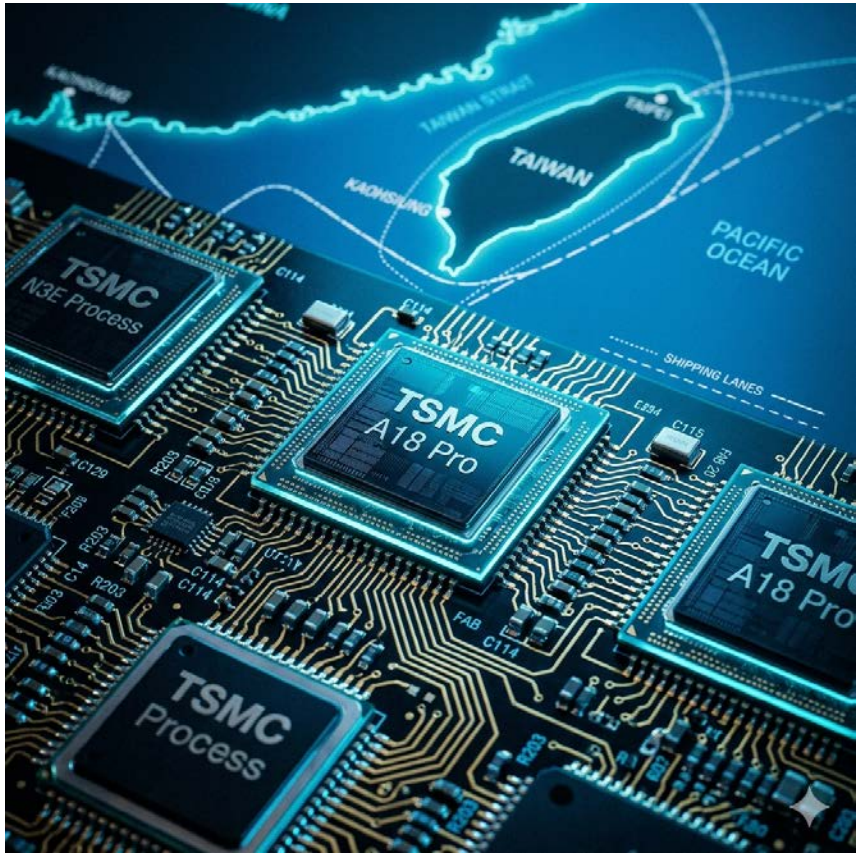
- Am 25. Dezember 2024 zerstörte der Anker eines Tankers das Seekabel Estlink 2.
- Die Kapazität fiel um 66%, Reparatur erst im Juni 2025.
- Vier Telekommunikationskabel wurden bei demselben Vorfall beschädigt.
- **Die Straße von Hormus** ist seit Februar 2026 gesperrt, der Verkehr liegt 95 Prozent unter Normal.
- Rund 20.000 Seeleute und 2.000 Schiffe nicht nur mit Öl liegen im Persischen Golf fest.

Welche Energieverträge halten einer Force-Majeure-Lage überhaupt stand?

Technologie

Ein Exportverbot entscheidet über die Versorgung mit zwei Elementen

- **China** verbot am 3. Dezember 2024 die Ausfuhr von Gallium, Germanium und Antimon in die USA.
- 94 Prozent des Galliums und 83 Prozent des Germaniums kommen aus China.
- Germanium hat sich seit 2023 um 211 Prozent verteuert, Gold um 124 Prozent.
- **In Baltimore** rammte im März 2024 ein Containerschiff die Brücke und der Hafen war wochenlang gesperrt.
- **Bei TSMC** wurden beim Erdbeben in Taiwan im April 2024 rund 60.000 Wafer beschädigt.



Gibt es Rohstoffe oder Bauteile nur in einer einzigen Quelle?

Ernährung und Landwirtschaft

Sechs Monate keine Auslieferung

- **Bei Asahi** stoppte am 29. September 2025 ein Ransomware-Angriff alle sechs japanischen Werke.
- Erst ab April 2026 lieferte das Unternehmen wieder vollständig aus, der Gewinn sank um 26 Prozent.
- **In Italien** lag im Sommer 2026 die Dürre über 60 Prozent der Landesfläche, beim Mais fiel bis zu 70 Prozent der Ernte aus.
- Der Kakaopreis stieg im April 2024 so stark wie nie seit Beginn der Aufzeichnungen 1963.
- Im August 2026 brauchte dieselbe Ladung wegen Niedrigwasser sieben Schiffe statt zwei.
- **In Odessa** lagen im Juli 2026 elf Millionen Tonnen Getreide ohne Lagerplatz.

Wie viele Tage Verzug verträgt eine kritische Infrastruktur?

Immobilien und Bau

Baustoffe kommen aus dem Ausland

- Von Stahl über Holz bis zur Fliese wird ein großer Teil der Baustoffe importiert.
- Zement und Zuschlagstoffe hängen am Binnenschiff und damit am Wasserstand.
- **Im August 2026** stiegen die Frachten in den Rhein-Seehafen-Verkehren um 100 bis 120 Prozent.
- **In Valencia** zerstörte die Flut im Oktober 2024 Infrastruktur und band Baukapazität.
- Verzögert sich ein Bau, verzögert sich auch die erste Mieteinnahme.
- Kalkulationen aus der Planungsphase halten nicht und Investitionen erreichen ihre Grenze.

Welches Projekt kennt heute schon den Ursprung seiner Baustoffe?

„Die Zahl“ und wo wir helfen können

26.225 Störungen im Jahr.

Für ein einzelnes Unternehmen zählt am Ende nur, dass es überlebt.

Wo wir ansetzen

- Eine Lieferkette überschreitet Grenzen, eine Beratung muss das auch
- Jeder Hinweis aus einem Land wird zum Vorteil für den Mandanten im nächsten
- Gemeinsame Mandate lassen alle Beteiligten wachsen

Warum gemeinsam

- Weil wir Moore Deutschland sind: über 1.000 Fachleute
- Und nah am Mandanten sind
- International: 119 Länder, 568 Standorte, mehr als 37.000 Fachleute im Moore-Netzwerk

Wachstum entsteht nicht daraus, die Krise vorherzusagen, sondern daraus, vorbereitet zu sein.

MOORE Deutschland

Vielen Dank

Markus Bitzer

Bitzer Mainfort GmbH

markus.bitzer@bitzer-mainfort.com

MOORE Deutschland

Risk Advisory Services

Pawel Kogan

Agenda

Komplexe regulatorische Anforderungen	01
COSO als Grundlage	02
ControlMark: Der IKS-Zyklus	03
Certinova: Die IKS-Validierung	04

Komplexe regulatorische Anforderungen

Anforderungen im Überblick

Regulierung und Standards
NIS 2, DORA, EU AI Act, ISO 42001, DSGVO/ESRS, CSRD, Außenwirtschaftsrecht und Exportkontrolle u.v.m.

Prüfung und Nachweise
SOC-Reports, IDW PS-Prüfungen (z.B. 951, 980-983), ISA 315 u.v.m.

Weitere Vorgaben
ISMS, Tax CMS, Nachhaltigkeit, interne Vorgaben, vertragliche Anforderungen u.v.m.

IKS

Internes Kontrollsystem

Struktur und Nachweisbarkeit

Anforderungen umsetzen und ihre Einhaltung nachweisen

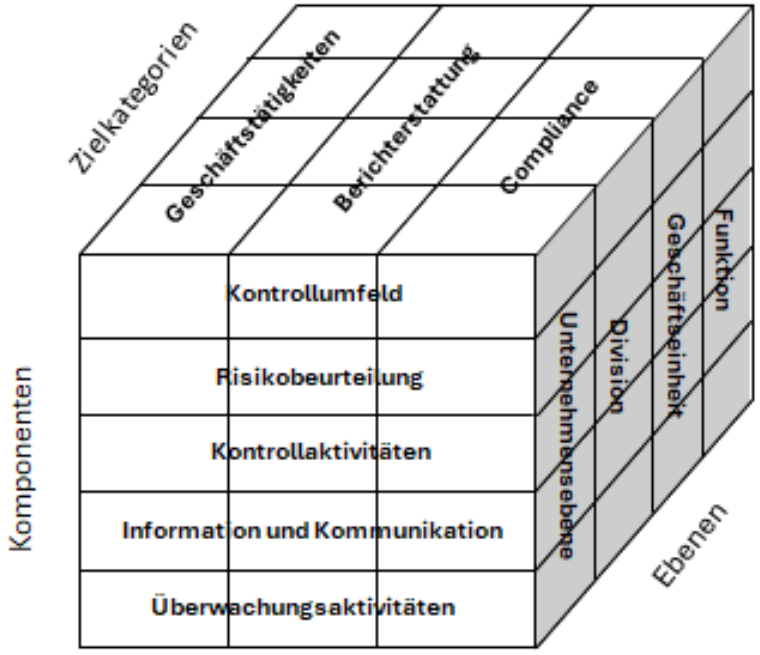
Steigende Erwartungen

Regulatoren, Prüfer, Kunden und Unternehmensorgane erwarten zunehmend belastbare Nachweise über die Einhaltung relevanter Anforderungen.

Lösung

- Ein strukturiertes IKS überführt unterschiedliche Anforderungen in Verantwortlichkeiten, Risiken, Kontrollen und Nachweise
- Certinova validiert Aufbau und Funktionsweise des IKS.

COSO als Grundlage



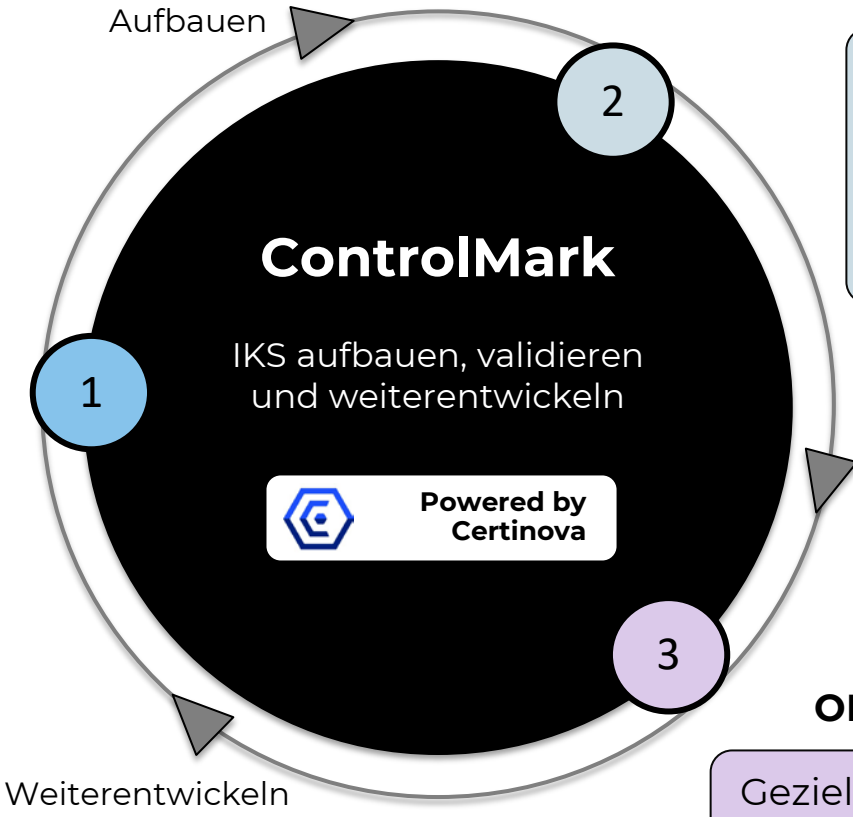
ZIELKATEGORIEN
Geschäftstätigkeit, Berichterstattung und Compliance definieren IKS-Ziele.

KOMPONENTEN
Die fünf COSO-Komponenten beschreiben, wie das IKS aufgebaut ist und umgesetzt wird.

EBENEN
Das IKS findet im gesamten Unternehmen Anwendung.

Ein IKS besteht nicht aus isolierten Kontrollen. Es ist ein **integriertes System**, das Zielkategorien, Komponenten und Organisationsebenen miteinander verbindet.

ControlMark: Der IKS-Zyklus



IKS-IMPLEMENTIERUNG

Struktur schaffen

Ziele, Verantwortlichkeiten, Risiken und Kontrollen festlegen.

EXTERNE VALIDIERUNG

Umsetzung bewerten

IKS-Ergebnisse durch Certinova anhand definierter Kriterien bewerten.

OPTIMIERUNG

Gezielte Verbesserung

Erkannten Optimierungsbedarf punktuell weiterbearbeiten.

Skalierbar | Digital validiert | Gemeinsam umgesetzt

Certinova: Die IKS-Validierung

01 PROBLEM

- Prüfungs- und Validierungsergebnisse sind für Dritte häufig nur eingeschränkt sichtbar.
- Nachweise und Berichte liegen in unterschiedlichen Formaten vor.
- Einordnung und Vergleichbarkeit der Ergebnisse sind schwierig.
- Interessensgruppen verfügen nur über begrenzte, leicht zugängliche Nachweise zur Prüfungs- und Kontrollqualität.

02 LÖSUNG

- Unabhängige, nachweisbasierte Validierungen und Prüfungen
- Strukturierte Beurteilung nach anerkannten Standards
- Klarer Bericht und nachvollziehbares Testat
- Differenzierte Badges für die IKS-Validierung
- Einheitlicher Badge für weitere Prüfungsleistungen

VALIDIERUNG UND TESTIERUNG

01 Aufbauprüfung

Beurteilung der Angemessenheit des Kontrollaufbaus

02 Funktionsprüfung

Beurteilung der Funktionsfähigkeit im laufenden Betrieb

03 Weitere Prüfungen und Testate

Einheitliches Badge für weitere unabhängige Prüfungsleistungen

MOORE Deutschland

VIELEN DANK FÜR DIE AUFMKERSAMKEIT!

Werbung!

Mitte November
veranstalten Aurélie Kleber (Coffra Group)
und Dr. Finn Martensen (Moore BRL)
ein
Webinar zu deutsch-französischen Verrechnungspreisthemen

Die Anmeldung ist via LinkedIn-Post von BRL möglich.
Oder Sie sprechen Dr. Finn Martensen einfach hier auf der Tagung an ☺


MOORE Deutschland
Mittagessen in „Die Wirtschaft“
Wir treffen uns wieder hier um 14:15 Uhr

MOORE Deutschland

Ein Cybervorfall, viele Learnings

Herbert Huber

MOORE Deutschland

Ein Cybervorfall, viele Learnings

Bericht aus der Praxis | 10. September 2026

Herbert Huber | Moore Salzburg

Die wichtigsten Angriffsmuster

Bedrohungen im Überblick

- Ransomware as a Service – arbeitsteilige Angriffe als Dienstleistung
- Double Extortion – Verschlüsselung plus drohende Veröffentlichung
- Business E-Mail Compromise – manipulierte Rechnungen und Bankverbindungen
- CEO-Betrug und Phishing – Zeitdruck, Überweisungen, Zugangsdaten
- APT und Insider-Risiken – Spionage, Sabotage und Datenabfluss

Unser Vorfall: Mehrstufiger Ransomware-Angriff; wichtiger als die Täterbezeichnung ist die Angriffskette.

Chronologie: Der Angriff hatte Vorlauf

- 2. März – erster festgestellter unberechtigter Zugriff; Script platziert
- 17.–19. März – privilegierte Konten, RDP-Zugriffe, Endpoint-Protection deaktiviert
- 19.–23. März – weitere Zugriffs- und Kontrollaktivitäten
- 1. April – Verschlüsselung und Erpresserschreiben

Learning: Der sichtbare Schaden war der Endpunkt einer längeren Kompromittierung.

Erste Reaktion und Krisenorganisation

1. Schaden begrenzen – Systeme isolieren und Verbindungen kontrolliert trennen
2. Beweise sichern – nichts vorschnell bereinigen; Forensik und Dokumentation starten
3. Verantwortung bündeln – Krisenstab und klare Entscheidungen
4. Betrieb sichern – alternative Kommunikation und kontrollierte Wiederherstellung

Ziel: technische und organisatorische Handlungsfähigkeit gleichzeitig herstellen

Kommunikation ist eine Sicherheitsmaßnahme

- Zwei interne Informationskreise
- Krisenstab / Geschäftsführung / IT / Forensik: Fakten, offene Fragen, Entscheidungen, Risiken
- Mitarbeitende / Führungskräfte: klare Anweisungen, erlaubte Systeme, nächste Updates

Praxis: Mattermost war selbstgehostet, außerhalb der betroffenen RDP-Umgebung und nicht kompromittiert.

Learning: Nicht alles auf eine Karte setzen – auch nicht bei Krisenkommunikation. IT- und Kommunikationsexperten heranziehen

Formel: Was wissen wir? Was tun wir? Was soll die Gruppe jetzt tun? Wann kommt das nächste Update?

Prävention: Sicherheitslücken konsequent schließen

- Awareness und Phishing-Schutz
- MFA, getrennte Administratorkonten und minimale Rechte
- Kritische Patches priorisieren, Herstellerwarnungen überwachen, Penetrationstests einsetzen
- Getrennte beziehungsweise Offline-Backups; Wiederherstellung regelmäßig testen

Unser Vorfall: zuletzt verfügbarer Patch war installiert; der kritische Patch kam später.

Learning: Aktueller Patchstand bedeutet nicht kein Risiko – Erkennung, Begrenzung und Wiederherstellung bleiben nötig.

Incident Readiness und Risikomanagement als Chefsache

Notfallplan: Auslösekriterien, Rollen, Eskalation, alternative Kanäle, Wiederanlaufreihenfolge

Übung: Tabletop mit Geschäftsführung, IT, Forensik, Datenschutz und Kommunikation

Risikomanagement: kritische Prozesse, Abhängigkeiten, Daten und Ausfallzeiten bewerten

Chefsache: Entscheidungen, Ressourcen, Verantwortlichkeiten und akzeptiertes Restrisiko festlegen

Ein geübter Plan begrenzt Ausfall und finanziellen Schaden.

Ransomware-Verhandlungen: Strategien gegen die digitale Erpressung

Erste Frage: Sind wir ohne Zahlung handlungsfähig?

1. Erpresserschreiben sichern, Systeme isolieren
2. Forensik: Verschlüsselung und möglicher Datenabfluss klären
3. Wiederherstellung und manuelle Ersatzprozesse bewerten
4. Geschäftsführung, Recht, Datenschutz, Strafverfolgung und Versicherer einbeziehen

Keine unkoordinierte Eigenverhandlung; keine Zahlung ohne rechtliche und sanktionsrechtliche Prüfung

Wiederherstellungsfähigkeit ist der wichtigste Verhandlungsvorteil.

Die wichtigsten Learnings

- Der sichtbare Schaden ist oft nur der Endpunkt.
- Erkennung und Berechtigungsmanagement zusammendenken
- Schutzsysteme gegen Manipulation schützen; Alarme bearbeiten
- Backups trennen, schützen und tatsächlich wiederherstellen können
- Krisenkommunikation unabhängig von kompromittierter IT organisieren
- Notfallplan, Rollen, alternative Kanäle und Übungen verankern
- Wiederherstellungsfähigkeit als Verhandlungsvorteil sichern

Was sollte jedes Unternehmen vorbereiten?

- Notfallkontakte und Eskalationskette aktualisieren
- Getrennte Kommunikationswege einrichten und testen
- Privilegierte Konten und Fernzugriffe überprüfen
- Wiederherstellung eines kritischen Systems praktisch testen
- Tabletop-Übung mit Geschäftsführung, IT, Datenschutz und Kommunikation durchführen
- Maßnahmen mit Verantwortlichen und Fristen nachverfolgen

Resilienz statt Sicherheitsillusion

Kein Einzelmittel schützt allein.

Cyberresilienz entsteht aus:

- technischen Schutzmaßnahmen
- kontrollierten Berechtigungen
- verlässlichen Sicherungen
- geübten Abläufen
- klarer Kommunikation

Ziel: früh erkennen, Schaden begrenzen, handlungsfähig bleiben, kontrolliert wiederherstellen.

Cyber-Resilienz: Lehren aus einem Ransomware-Angriff

Cyber-Sicherheit ist eine Managementaufgabe – über technische Patches hinaus, mit proaktiver Krisenplanung.

Die Anatomie des Angriffs: 30 Tage bis zum Stillstand

Vier Wochen unsichtbare Infiltration

Vom ersten Script am 2. März bis zur Verschlüsselung am 1. April vergingen 30 Tage.

Der Schaden ist nur der Endpunkt

Angreifer deaktivieren Schutzsysteme und übernehmen Konten lange vor der eigentlichen Erpressung.

Sofortige Isolation & Forensik

Systeme kontrolliert trennen, aber Beweise für die Analyse sichern, statt vorschnell zu löschen.

Strategien für echte Cyber-Resilienz

Kommunikation als Sicherheitsmaßnahme

Nutzen Sie externe, nicht kompromittierte Kanäle für Krisenstab und Belegschaft.

Wiederherstellung ist der beste Schutz

Offline-Backups und geübte Recovery-Prozesse sind der wichtigste Vorteil in Ransomware-Verhandlungen.

Resilienz ist Chefsache

Notfallpläne, Tabletop-Übungen und Ressourcenfestlegung liegen in der Verantwortung der Geschäftsführung.

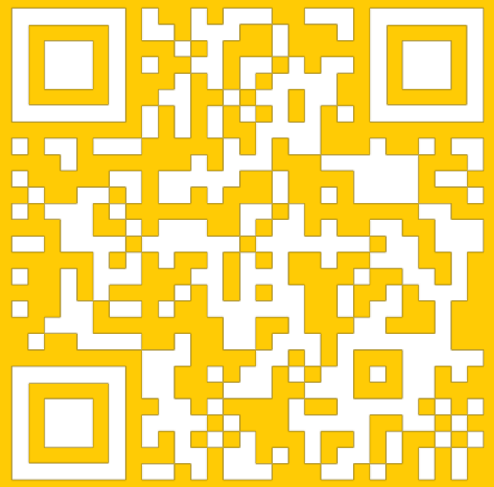
Vergleich: Technischer Stand vs. Tatsächliches Risiko

STATUS	REALITÄT	KONSEQUENZ
Patchstand aktuell	Kritischer Patch fehlte noch	Patching allein ist kein 100% Schutz
Backup vorhanden	Wiederherstellung ungeübt	Ausfallzeit und finanzieller Schaden steigen
IT-Schutz aktiv	Durch Angreifer deaktiviert	Überwachung von Admin-Konten ist kritisch

MOORE Deutschland

Herbert Huber

Moore Salzburg



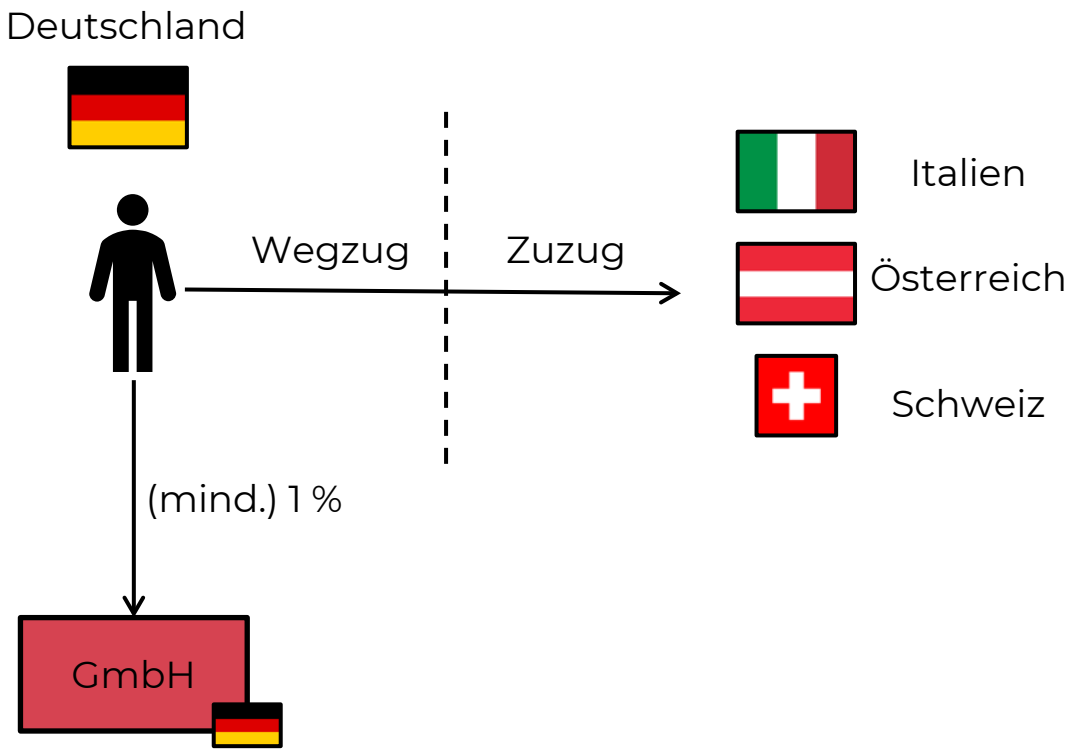
MOORE Deutschland

Grenzen überschreiten, Steuern beachten: Wegzug, Zuzug und steuerliche Standortwahl im DACHI-Raum

Christian Schöler, Raimondo Salis, Hannes Kofler,
Michael Brightwell, Melanie Gomringer

Moore Deutschland Jahrestagung 2026 in Nürnberg

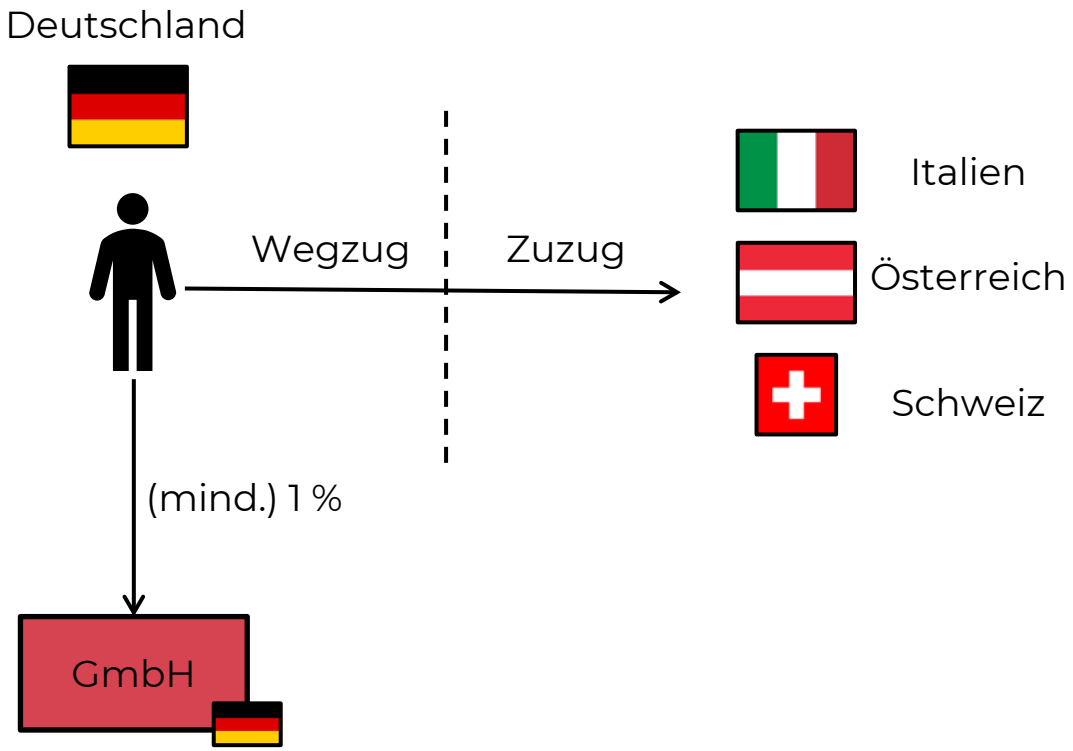
Ausgangssachverhalt



Sachverhalt

- Ein in Deutschland unbeschränkt Steuerpflichtiger hat seinen Wohnsitz in Deutschland
- Steuerpflichtiger ist zu (mindestens) 1 % an einer deutschen GmbH beteiligt
- Die deutsche GmbH erzielt Einkünfte aus operativer Tätigkeit
- Der Steuerpflichtige gibt seinen Wohnsitz in Deutschland dauerhaft auf
- Zuzug nach ITALIEN/ÖSTERREICH/ SCHWEIZ

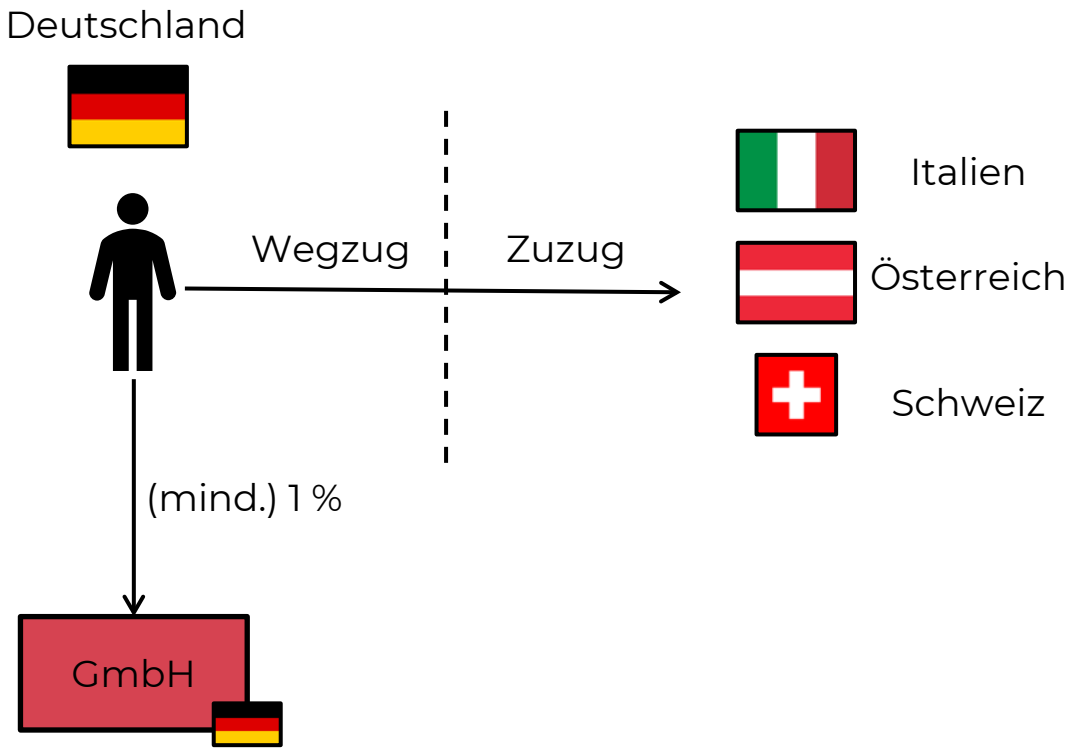
Ausgangssachverhalt



Deutschland

- Wird eine Wegzugsbesteuerung ausgelöst?
  - Falls ja, wie wird der fiktive Veräußerungsgewinn ermittelt?
  - Welche Möglichkeiten zur Steuerstundung bestehen?
- Ort der Geschäftsleitung der GmbH?
- Sonstige Entstrickungsrisiken
- Erweitert beschränkte Steuerpflicht(-en)

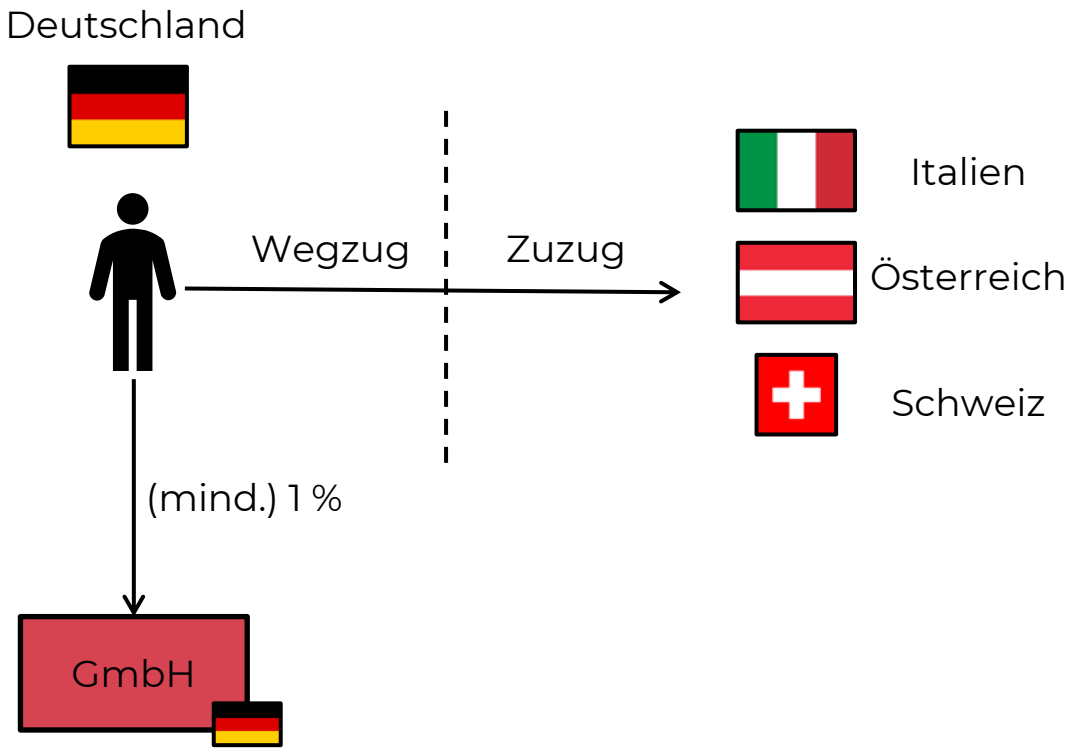
Ausgangssachverhalt



Zuzugsstaat

- Begründung der Steuerpflicht bzw. Ansässigkeit im Zuzugsstaat?
- Steuerliche Verhaftung der Beteiligung im Zuzugsstaat und Folgen für Dividende und / oder Anteilsverkäufe
  - Erfolgt ein steuerlicher Step-Up auf den Verkehrswert bei Zuzug?
  - Behandlung deutscher Wegzugsteuer im Zuzugsstaat
- Exit-Besteuerung bei Rück- bzw. „Weiterzug“?

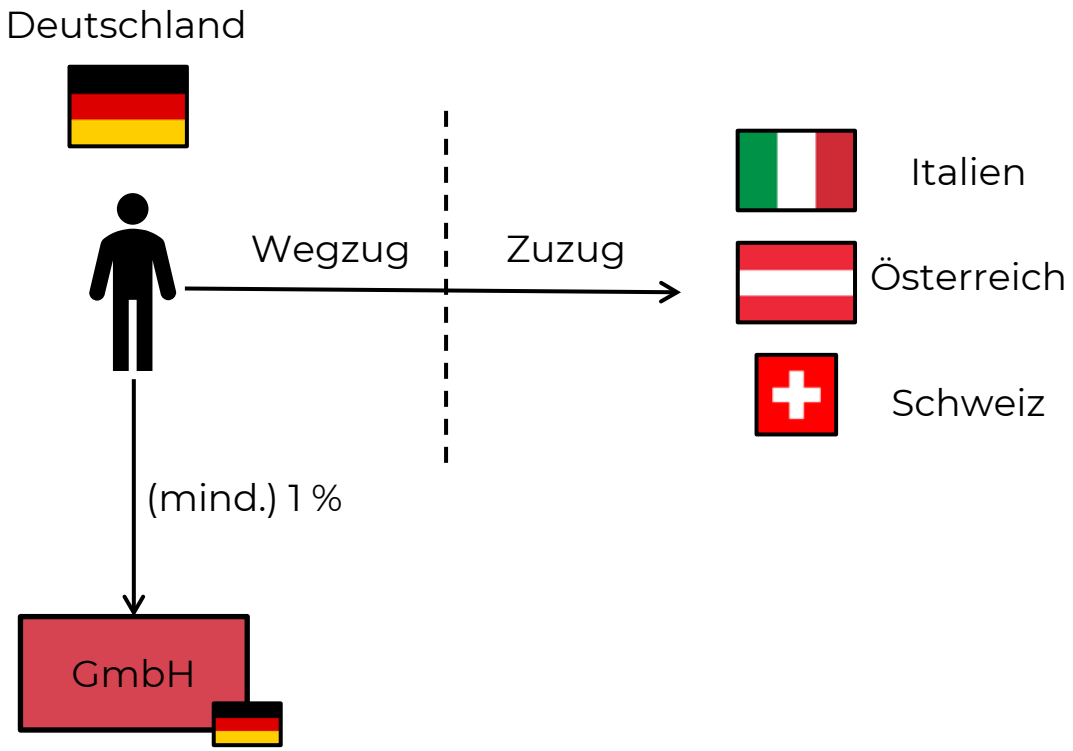
Ausgangssachverhalt



Strukturierungsmöglichkeiten, u.a.

- (Temporäre Abwesenheit)
- Formwechsel der GmbH
- Stiftungslösungen
- GmbH & Co. KG als Holding
- Schenkung an Abkömmlinge (sofern in DE ansässig)

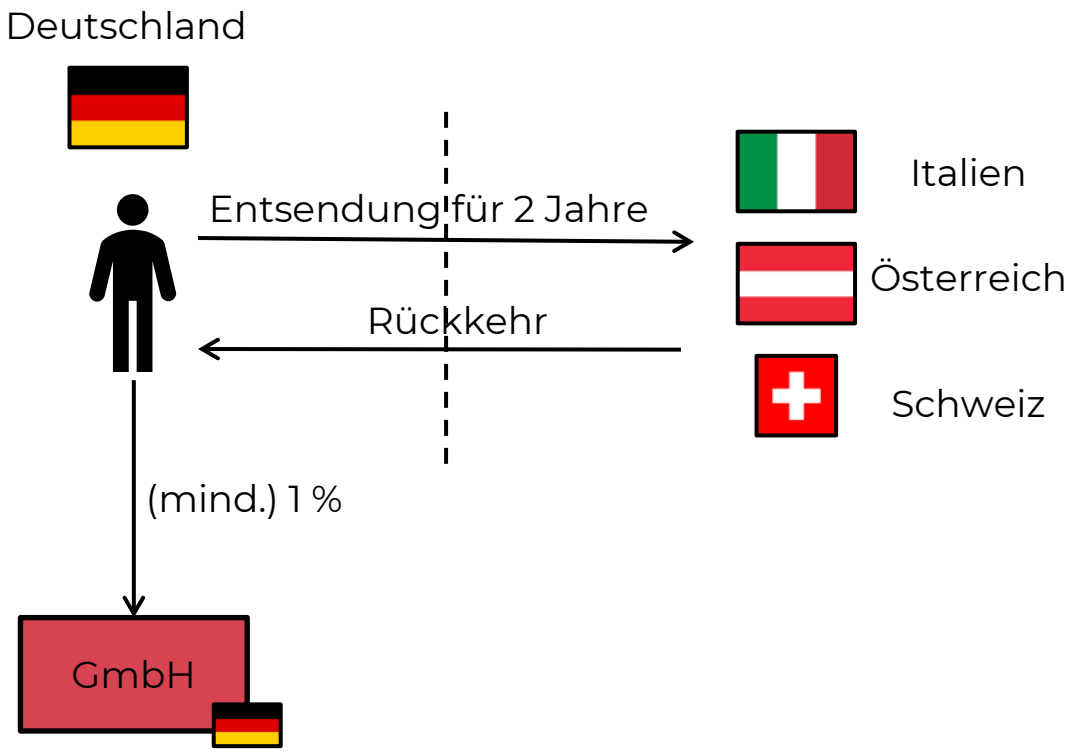
Ausgangssachverhalt



Special Tax Regimes

- Steuerliche Vorteile für Neu-Zuziehende
- Besonderheiten in den Sonderregimen
- Knüpfung steuerlicher Begünstigungen an Mindestinvestitionen?
- Anforderungen hinsichtlich Höhe und Zusammensetzung des Vermögens und Folgen des Verstoßes
- Beschränkungen hins. Anlageformen / Beteiligungshöhe
- Beachte: erweitert beschränkte Steuerpflicht § 2 AStG

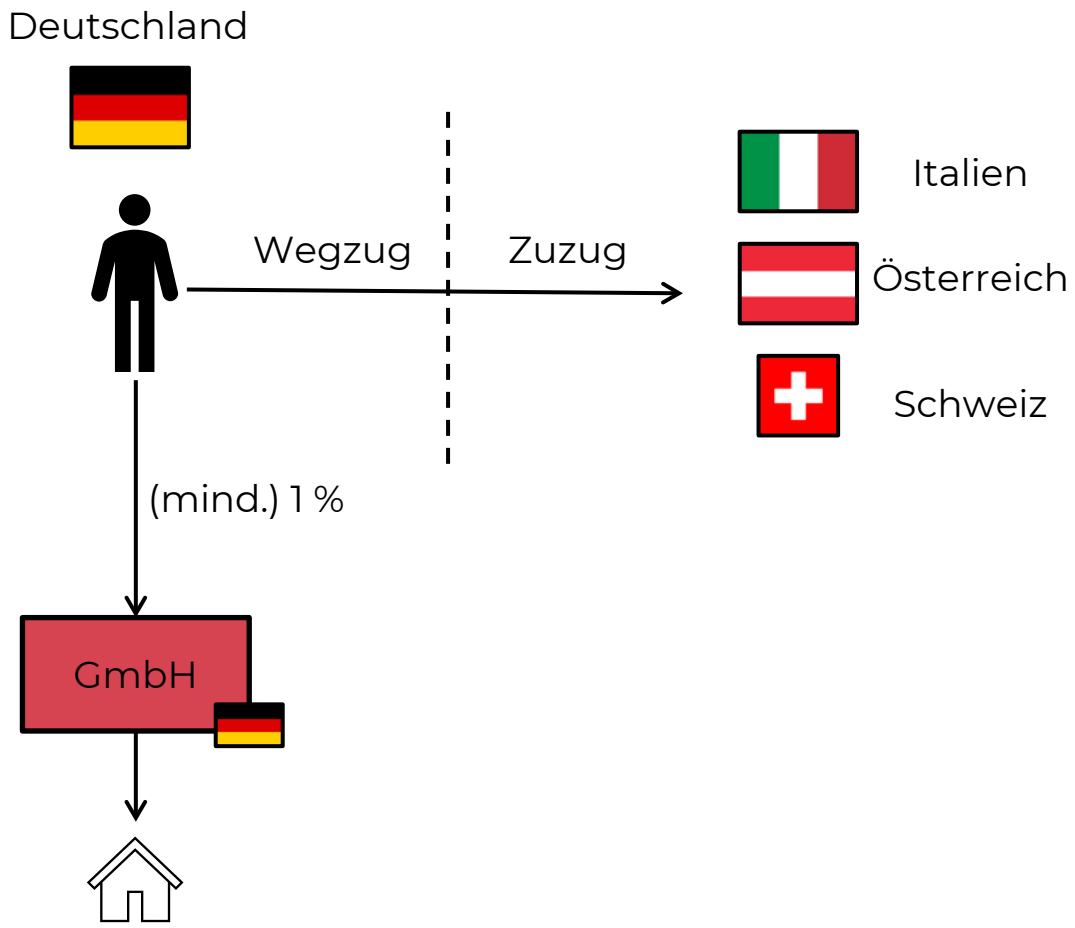
Abwandlung Entsendung



Sachverhalt

- Ein in Deutschland unbeschränkt Steuerpflichtiger hat seinen Wohnsitz in Deutschland
- Er ist zu (mindestens) 1 % an einer deutschen GmbH beteiligt und ist gleichzeitig bei der deutschen GmbH angestellt
- Im Rahmen der Anstellung wird der Steuerpflichtige nach ITALIEN/ÖSTERREICH/ SCHWEIZ entsandt
- Entsendung ist zeitlich befristet auf zwei Jahre
- Nach Entsendung kehrt der Steuerpflichtige nach Deutschland zurück

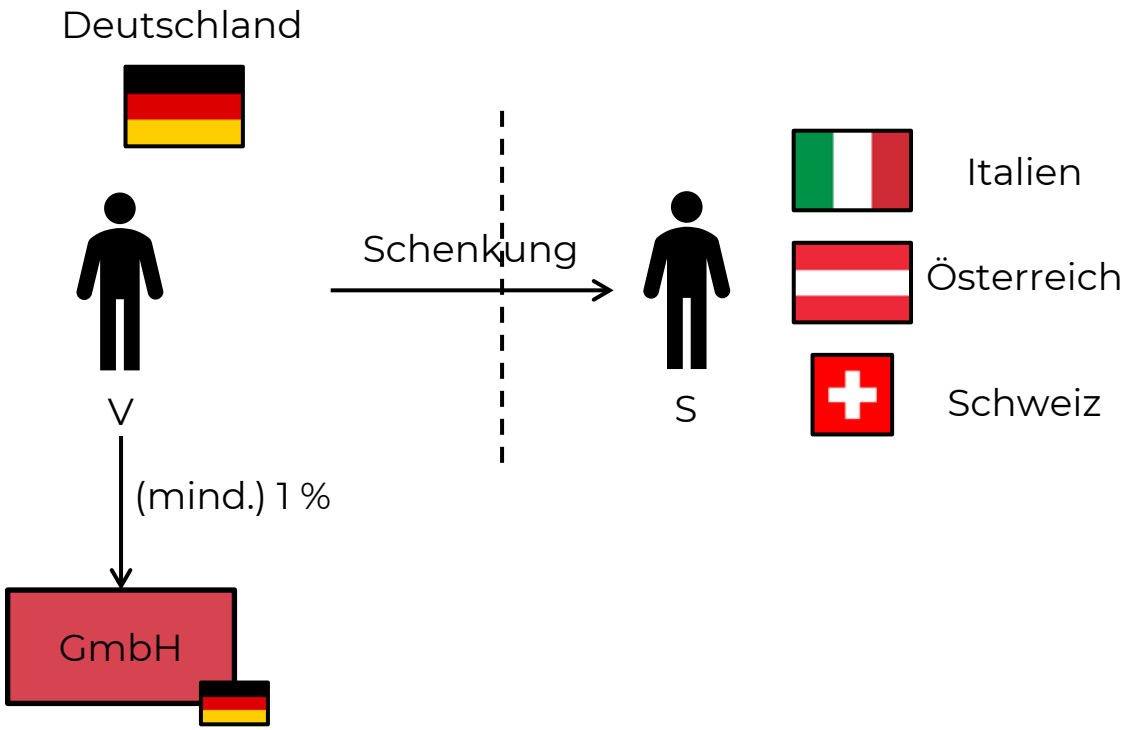
Abwandlung Immobiliengesellschaft



Sachverhalt

- Ein in Deutschland unbeschränkt Steuerpflichtiger hat seinen Wohnsitz in Deutschland
- Er ist zu (mindestens) 1 % an einer deutschen GmbH beteiligt
- Die GmbH hält überwiegend Immobilienvermögen
- Zuzug nach ITALIEN/ÖSTERREICH/ SCHWEIZ unter Beibehaltung des deutschen Wohnsitzes

Abwandlung Erbschaft-/Schenkungsfall



Sachverhalt

- Der in Deutschland unbeschränkt steuerpflichtige V hat seinen Wohnsitz in Deutschland
- V hält eine Beteiligung an einer deutschen GmbH
- Sein Sohn S hat seinen Wohnsitz in ITALIEN / ÖSTERREICH / SCHWEIZ
- GmbH-Anteil gehen im Wege einer Erbschaft bzw. Schenkung auf S über

Ihre Ansprechpartner

Christian Schöler

Partner
Steuerberater
Christian.schoeler@sonntag-partner.de
T: +49 911 81511 475
M: +49 162 2867803

Dr. Michael Brightwell

Partner
Steuerberater
m.brightwell@mooreconnect.at
T: +43 1 602 02 02
M: +43 676 973 02 20

Raimondo Salis

Partner Tax / Legal
dipl. Steuerexperte
raimondo.salis@moore-zurich.com
T: +41 44 828 18 18

Melanie Gomringer

Mandatsleiterin Tax / Legal
MAS Swiss and International Taxation
melanie.gomringer@moore-zurich.com
T: +41 44 828 18 18

Hannes Kofler, LL.M.

Partner
WP/Steuerberater
hannes.kofler@bureauplattner.com
T: +39 0471 222500
M: +39 348 64 03 116

MOORE Deutschland

Verabschiedung

Thomas Ziegler

MOORE Deutschland

Vielen Dank,
eine gute Heimreise
und bis nächstes Jahr
in Göttingen!