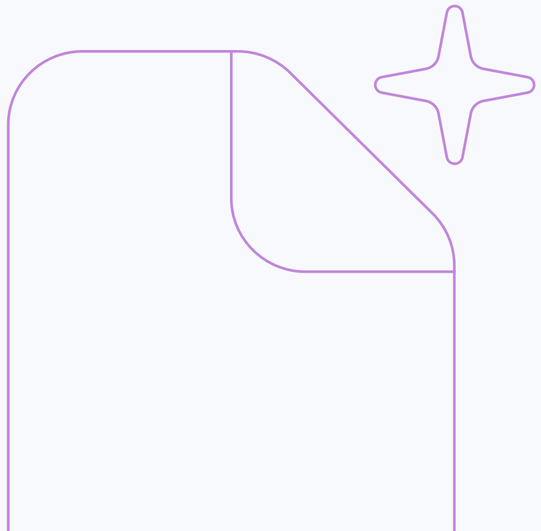
06.02.2026

Wie KI und Automatisierung bei Multi-Framework Compliance unterstützen

60. Sitzung der Denkfabrik Legal Tech
zum Thema „Digital Compliance“



Herausforderung

Ein Gesetzestext kommt selten allein.

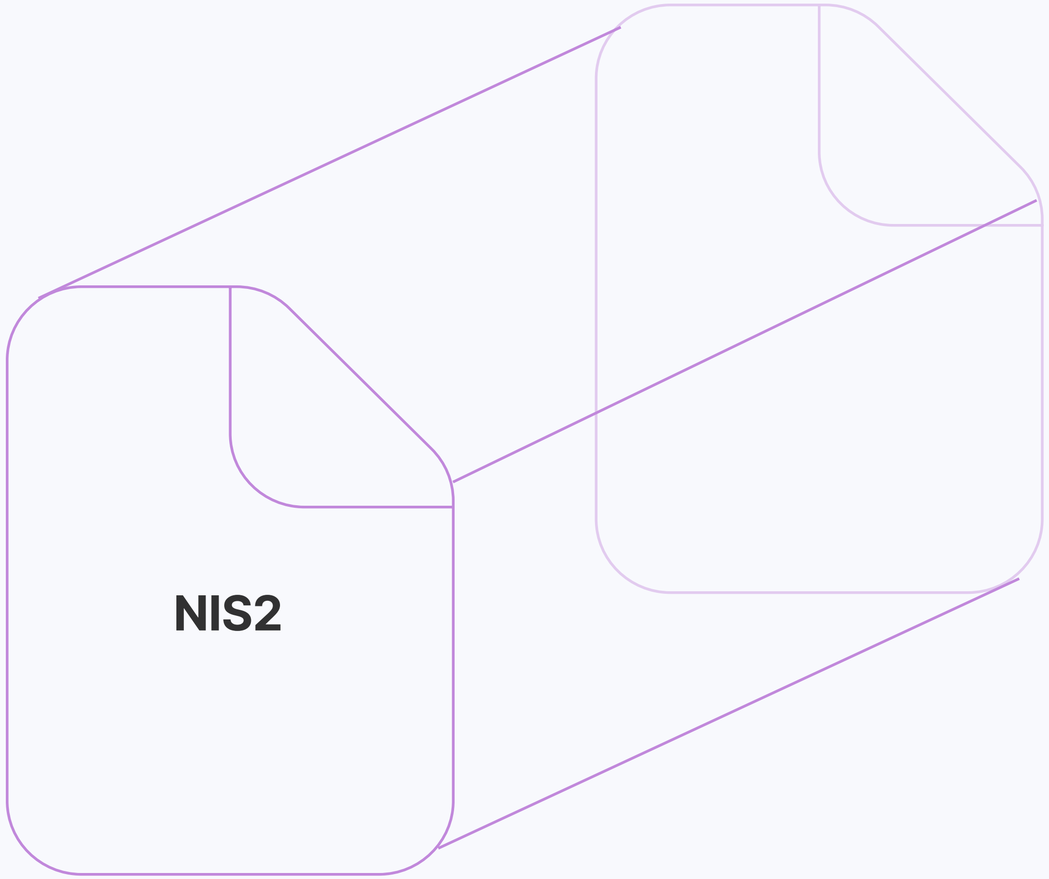
Die Compliance-Anforderungen an Unternehmen steigen stetig.

kertos

Herausforderung

Wie bleibt man compliant bei neuen Gesetzen?

NIS2 ist da - rund 30.000 deutsche Unternehmen müssen jetzt verstehen, wie sie ein fast 70-seitiges Dokument mit rund 25.000 Wörtern in die Praxis umsetzen, um Strafen zu vermeiden.

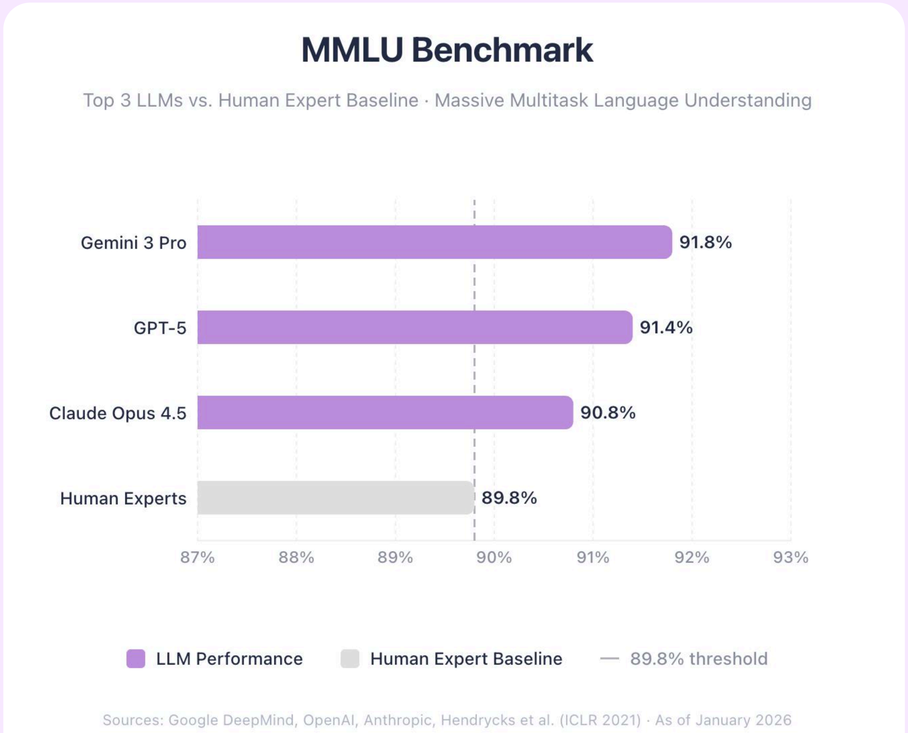


kertos

Lösung

Warum KI als Hilfsmittel?

Top LLMs outperformen menschliche Experten im Massive Multitask Language Understanding Test.

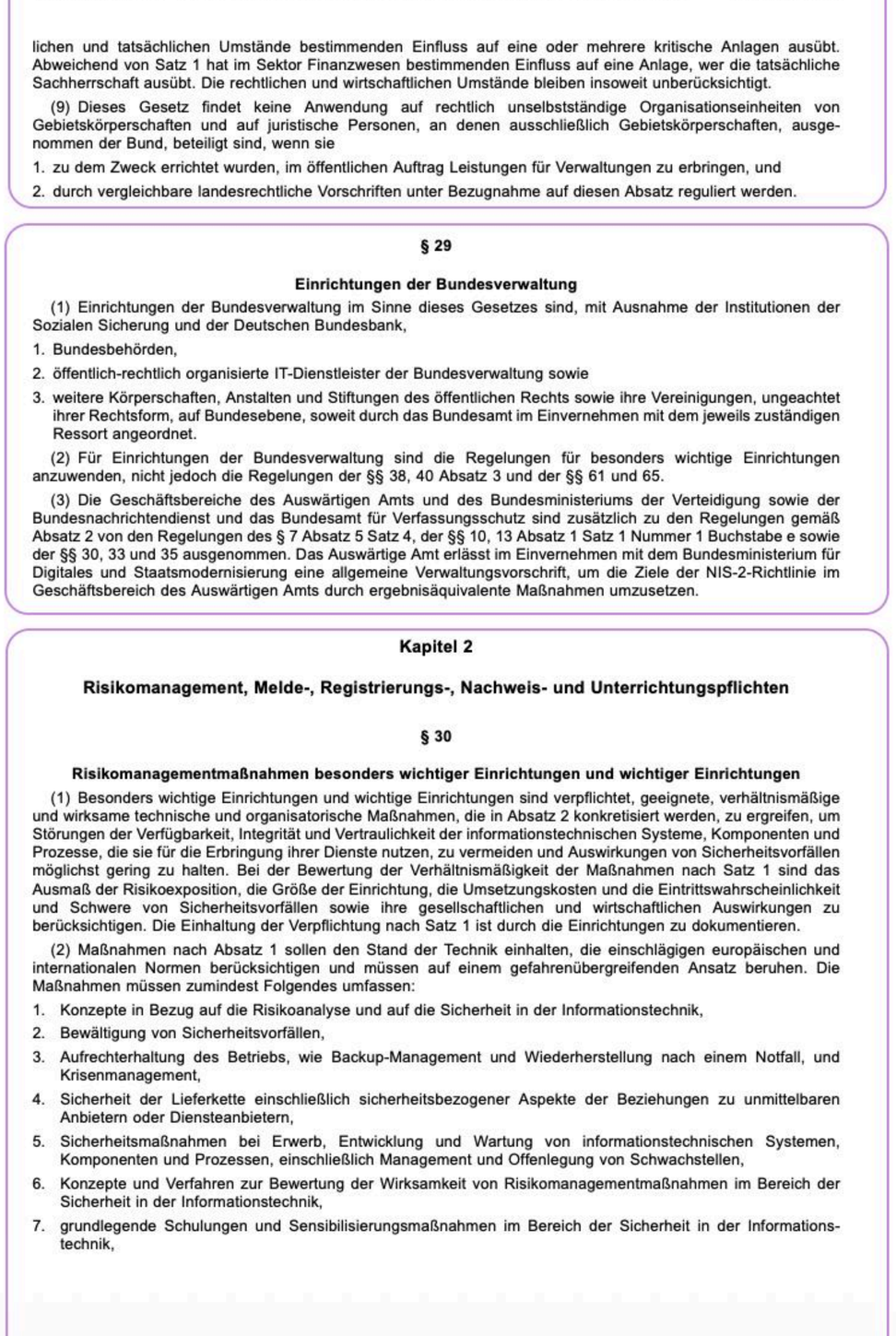


kertos

Analyse

Jedes Dokument ist anders.

- Eigene Gliederung
- Eigene Terminologie & Sprachgebrauch
- Informative vs. normative Teile
- ...



lichen und tatsächlichen Umstände bestimmenden Einfluss auf eine oder mehrere kritische Anlagen ausübt. Abweichend von Satz 1 hat im Sektor Finanzwesen bestimmenden Einfluss auf eine Anlage, wer die tatsächliche Sachherrschaft ausübt. Die rechtlichen und wirtschaftlichen Umstände bleiben insoweit unberücksichtigt.

(9) Dieses Gesetz findet keine Anwendung auf rechtlich unselbstständige Organisationseinheiten von Gebietskörperschaften und auf juristische Personen, an denen ausschließlich Gebietskörperschaften, ausgenommen der Bund, beteiligt sind, wenn sie

1. zu dem Zweck errichtet wurden, im öffentlichen Auftrag Leistungen für Verwaltungen zu erbringen, und
2. durch vergleichbare landesrechtliche Vorschriften unter Bezugnahme auf diesen Absatz reguliert werden.

§ 29

Einrichtungen der Bundesverwaltung

(1) Einrichtungen der Bundesverwaltung im Sinne dieses Gesetzes sind, mit Ausnahme der Institutionen der Sozialen Sicherung und der Deutschen Bundesbank,

1. Bundesbehörden,
2. öffentlich-rechtlich organisierte IT-Dienstleister der Bundesverwaltung sowie
3. weitere Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihre Vereinigungen, ungeachtet ihrer Rechtsform, auf Bundesebene, soweit durch das Bundesamt im Einvernehmen mit dem jeweils zuständigen Ressort angeordnet.

(2) Für Einrichtungen der Bundesverwaltung sind die Regelungen für besonders wichtige Einrichtungen anzuwenden, nicht jedoch die Regelungen der §§ 38, 40 Absatz 3 und der §§ 61 und 65.

(3) Die Geschäftsbereiche des Auswärtigen Amts und des Bundesministeriums der Verteidigung sowie der Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz sind zusätzlich zu den Regelungen gemäß Absatz 2 von den Regelungen des § 7 Absatz 5 Satz 4, der §§ 10, 13 Absatz 1 Satz 1 Nummer 1 Buchstabe e sowie der §§ 30, 33 und 35 ausgenommen. Das Auswärtige Amt erlässt im Einvernehmen mit dem Bundesministerium für Digitales und Staatsmodernisierung eine allgemeine Verwaltungsvorschrift, um die Ziele der NIS-2-Richtlinie im Geschäftsbereich des Auswärtigen Amts durch ergebnisäquivalente Maßnahmen umzusetzen.

Kapitel 2

Risikomanagement, Melde-, Registrierungs-, Nachweis- und Unterrichtungspflichten

§ 30

Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen, die in Absatz 2 konkretisiert werden, zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Bei der Bewertung der Verhältnismäßigkeit der Maßnahmen nach Satz 1 sind das Ausmaß der Risikoexposition, die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen. Die Einhaltung der Verpflichtung nach Satz 1 ist durch die Einrichtungen zu dokumentieren.

(2) Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. Die Maßnahmen müssen zumindest Folgendes umfassen:

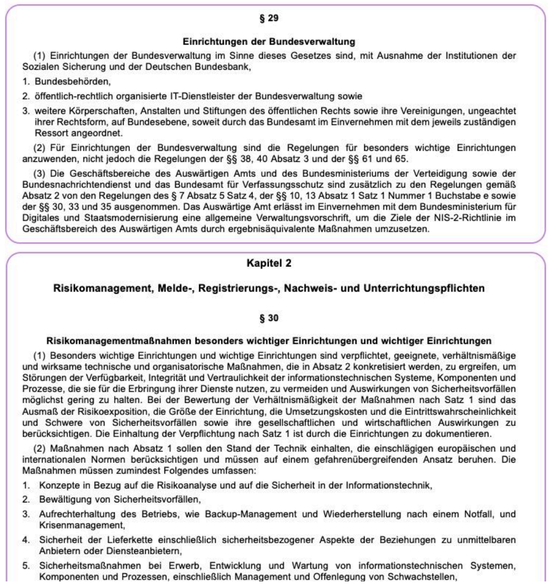
1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,
2. Bewältigung von Sicherheitsvorfällen,
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern,
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
7. grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik,

kertos

Zerlegung

Vom Urtext zu Anforderungen

Statt den Urtext auf einmal zu verarbeiten, iterieren wir mit dedizierten Subagenten über die einzelnen Abschnitte und identifzieren zunächst relevante Zitate und dann Anforderungen aus diesen Zitaten.



§ 29

Einrichtungen der Bundesverwaltung

(1) Einrichtungen der Bundesverwaltung im Sinne dieses Gesetzes sind, mit Ausnahme der Institutionen der Sozialen Sicherung und der Deutschen Bundesbank,

1. Bundesbehörden,
2. öffentlich-rechtlich organisierte IT-Dienstleister der Bundesverwaltung sowie
3. weitere Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihre Vereinigungen, ungeachtet ihrer Rechtsform, auf Bundesebene, soweit durch das Bundesamt im Einvernehmen mit dem jeweils zuständigen Ressort angeordnet.

(2) Für Einrichtungen der Bundesverwaltung sind die Regelungen für besonders wichtige Einrichtungen anzuwenden, nicht jedoch die Regelungen der §§ 38, 40 Absatz 3 und der §§ 61 und 65.

(3) Die Geschäftsbereiche des Auswärtigen Amts und des Bundesministeriums der Verteidigung sowie der Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz sind zusätzlich zu den Regelungen gemäß Absatz 2 von den Regelungen des § 7 Absatz 5 Satz 4, der §§ 10, 13 Absatz 1 Satz 1 Nummer 1 Buchstabe e sowie der §§ 30, 33 und 35 ausgenommen. Das Auswärtige Amt erlässt im Einvernehmen mit dem Bundesministerium für Digitales und Staatsmodernisierung eine allgemeine Verwaltungsvorschrift, um die Ziele der NIS-2-Richtlinie im Geschäftsbereich des Auswärtigen Amts durch ergebnisäquivalente Maßnahmen umzusetzen.

Kapitel 2

Risikomanagement, Melde-, Registrierungs-, Nachweis- und Unterrichtungspflichten

§ 30

Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen, die in Absatz 2 konkretisiert werden, zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Bei der Bewertung der Verhältnismäßigkeit der Maßnahmen nach Satz 1 sind das Ausmaß der Risikoexposition, die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen. Die Einhaltung der Verpflichtung nach Satz 1 ist durch die Einrichtungen zu dokumentieren.

(2) Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. Die Maßnahmen müssen zumindest Folgendes umfassen:

1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,
2. Bewältigung von Sicherheitsvorfällen,
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Dienstleistern,
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,

NIS2 (BSIG) Urtext

"Die Maßnahmen müssen umfassen: Aufrechterhaltung des Betriebs wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement"

Zitate

Die Maßnahmen müssen die Aufrechterhaltung des Betriebs umfassen.

Die Maßnahmen müssen eine Wiederherstellung nach einem Notfall umfass...

Die Maßnahmen müssen ein Krisenmanagement umfassen.

Anforderungen

kertos

Normalisierung

Anforderungs-Normalisierung

Um Anforderungen aus verschiedenen Gesetztestexten und Normen vergleichbar zu machen, verwenden wir unser selbst erstelltes Wörterbuch.

Prozesse und Verfahren zur Sicherstellung der Lieferkette müssen Dienstleister berücksichtigen.

Die Sicherheit der Lieferkette muss Beziehungen zu Dienstanbietern umfassen.

Dictionary

Prozesse und Verfahren zur Sicherstellung der Lieferkette müssen Lieferanten berücksichtigen.

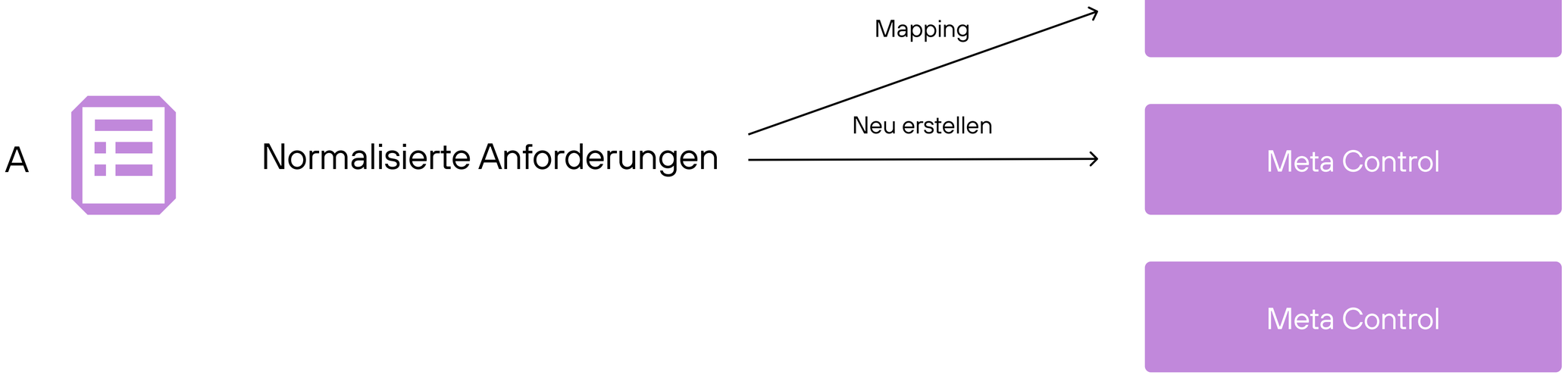
Die Sicherheit der Lieferkette muss Beziehungen zu Lieferanten umfassen.

kertos

Mapping & Erweiterung

Meta-Controls

Die normalisierten Anforderungen werden auf unser Verzeichnis von Meta-Controls gemapped oder neue Meta-Controls erstellt.

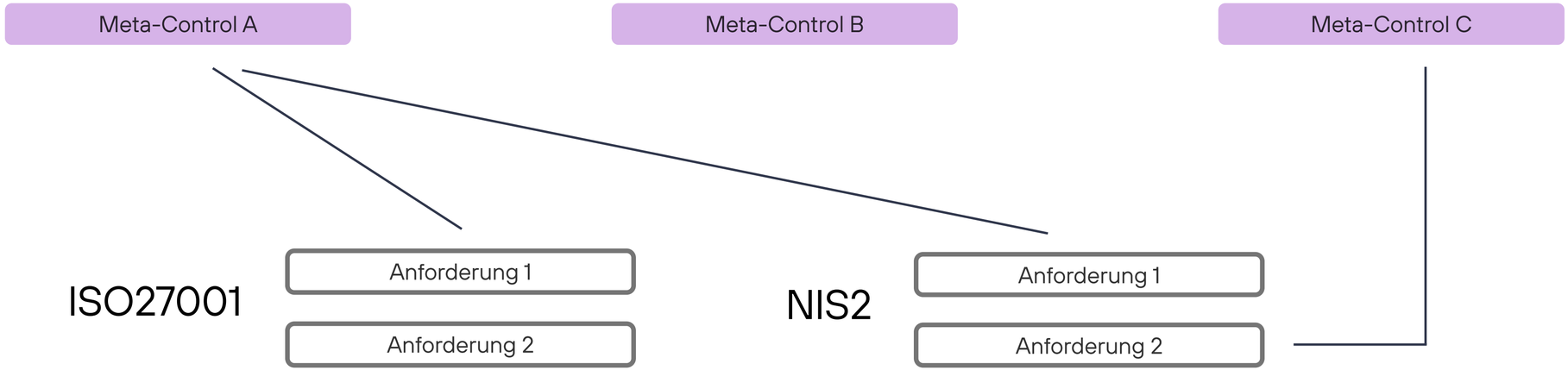


kertos

Mapping & Erweiterung

Was sind Meta-Controls?

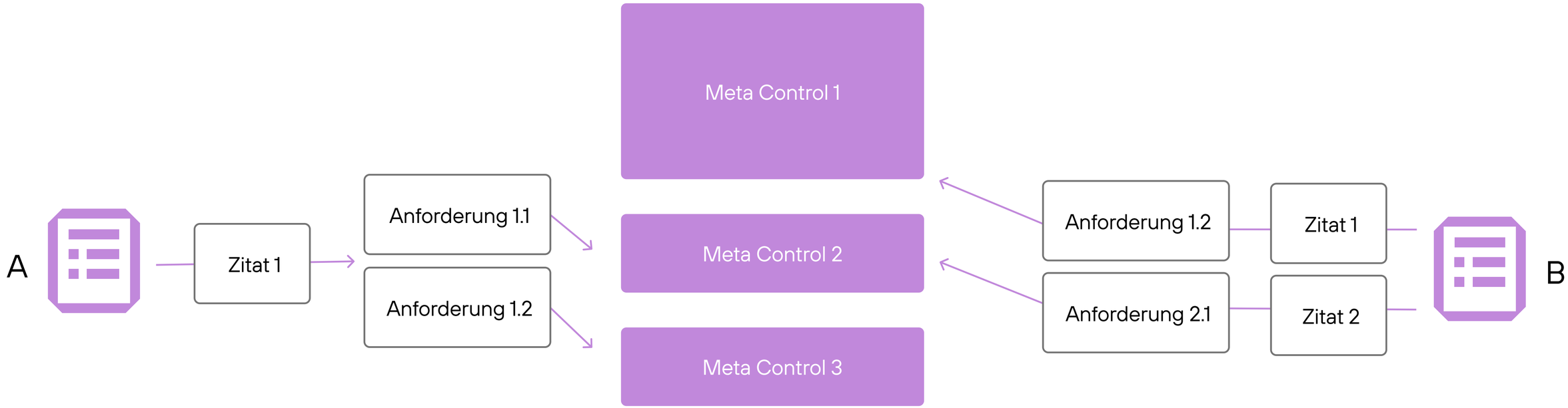
Meta-Controls sind von uns definierte Framework-übergreifende Maßnahmen, die gleichzeitigen Compliance-Fortschritt in verschiedenen Regulierungen & Standards ermöglichen.



Übersicht

Der komplette Prozess

Durch die Ableitung von Meta Controls mit der Hilfe von KI schaffen wir die Basis für die gleichzeitige Implementierung von Controls aus verschiedenen Frameworks.

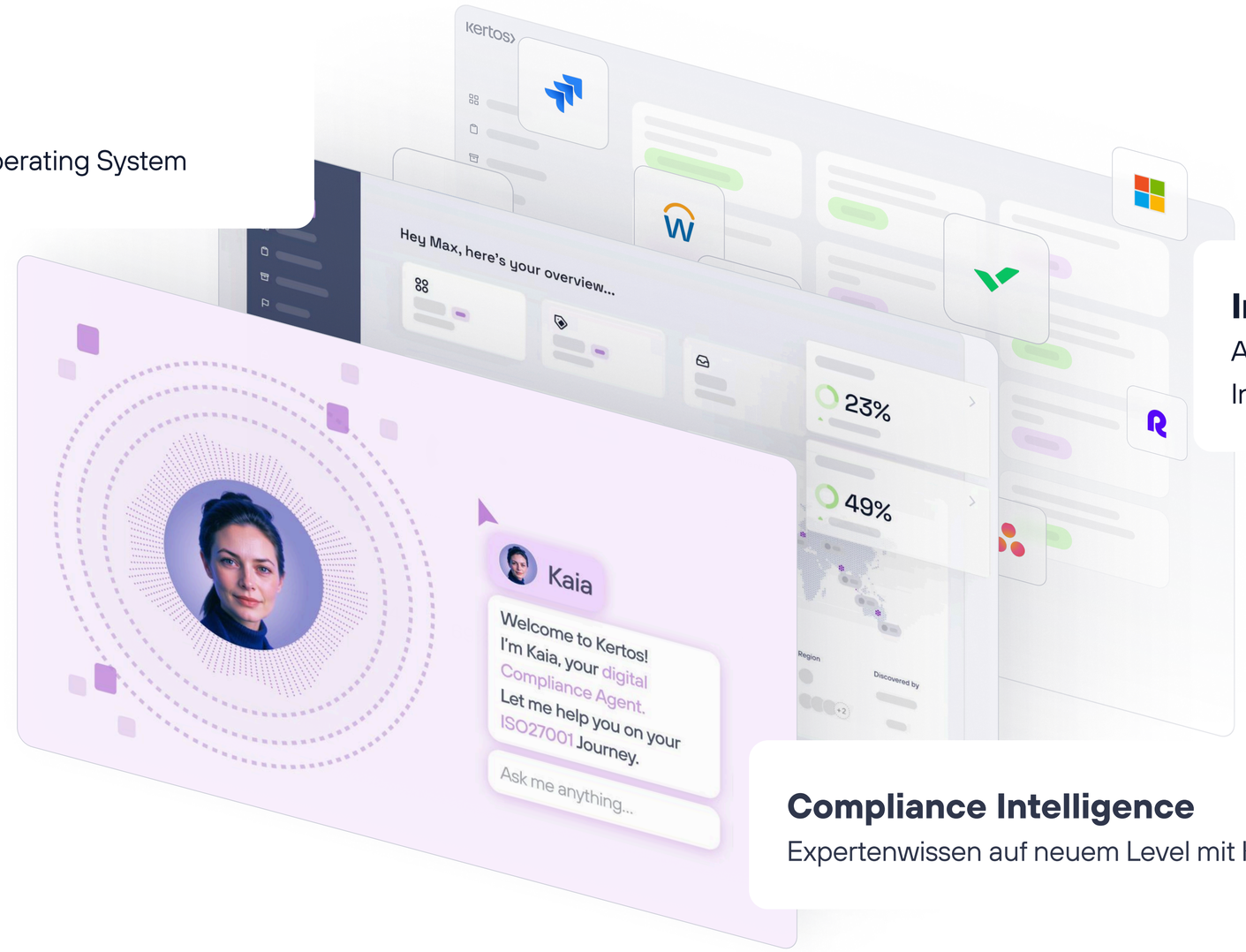


kertos

Die Zukunft der Compliance-Automatisierung

Kertos OS

Das Compliance Operating System



Integrationen

Alle compliance-relevanten Informationen in Echtzeit

Compliance Intelligence

Expertenwissen auf neuem Level mit KI

kertos

Wer wir sind

kertos>

Europas führende Compliance-Lösung.

Über 250 Unternehmen vertrauen uns bereits für die Compliance mit den wichtigsten Regulierungen und Zertifizierungen.

kertos>

GET IN TOUCH

Happy to get in touch

Your trusted partner in compliance, delivering expertise with integrity

Co-Founder

Johannes Hussak

johannes.hussak@kertos.io

kertos

Compliance First. Efficiency always.