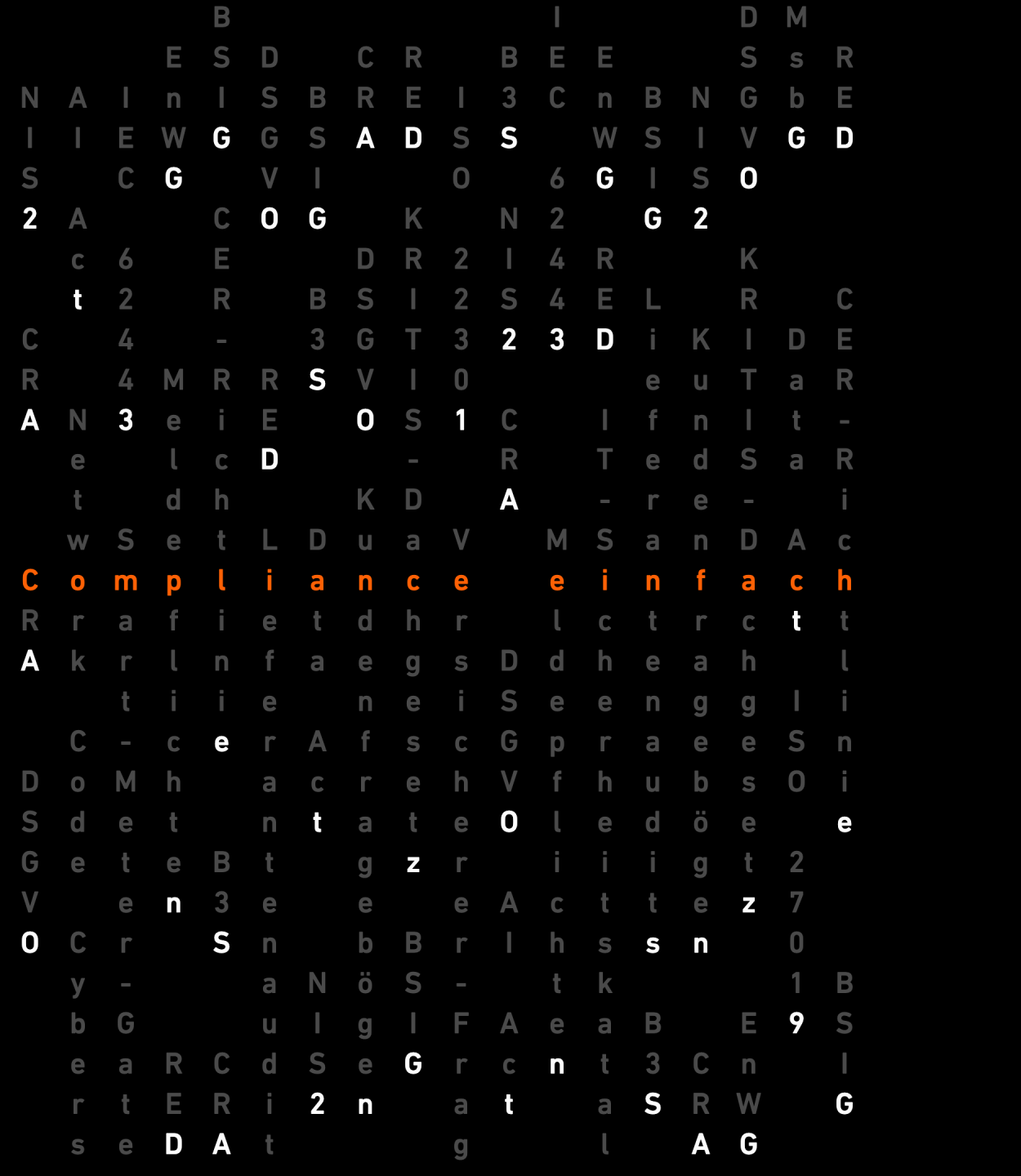
DENA KONGRESS 2026

Compliance? Einfach quer denken.

KRITIS, NIS2 & Co.: Wie Sie Compliance effizient und einfach umsetzen

David Fuhr · Mitgründer intcube.io

int[cube]



KURZE FRAGE AN SIE

Wer kann aus dem Stand sagen, welche Regelwerke für das eigene Unternehmen gelten?

Was alles gilt oder gerade kommt

Eine Auswahl für die Energiewirtschaft

NIS2 · IT-Sicherheitskatalog · BSI-KritisV · CRA · EN 18031 · KRITIS-Dachgesetz · DSGVO

MsbG · BSI TR-03109 · ISO 27001 · NIS2UmsuCG · RED · CER-Richtlinie · AI Act · IEC 62443

Data Act · ISO 27019 · Network Code Cybersecurity · BSIG · ISO 22301 · IT-Grundschutz · B3S · EnWG

Kundenfragebögen · Lieferantenaudits · Versicherer-Fragebögen · Meldepflichten

int[cube]

Ein Vorfall, drei Meldewege.

Einzeln sinnvoll, zusammen einfach viel.

Regelwerk	Erste Meldung	Meldung	Abschluss	An wen
NIS2 (erheblicher Vorfall)	24 h	72 h	1 Monat	BSI
CRA (ausgenutzte Schwachstelle)	24 h	72 h	14 Tage nach Fix	CSIRT und ENISA
DSGVO (Datenpanne)	-	72 h	-	Datenschutzaufsicht

Mit Pech 1 Vorfall -> 3 Fristen, 3 Stellen, 3 Formulare.

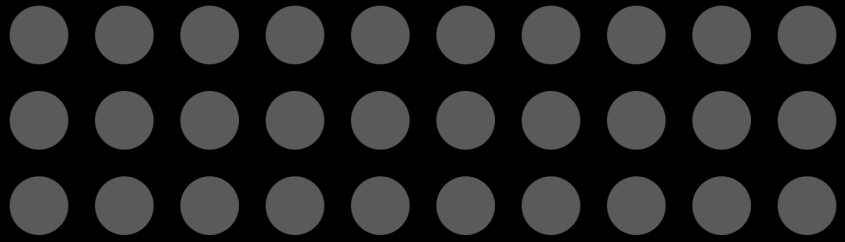
int[cube]

Ähnliche Pflichten, ein Bruchteil der Ressourcen.

Der Aufwand wächst, gerade für die kleinen Player.

Konzern

Compliance, Recht, Security, Revision, Datenschutz



Kleines Stadtwerk

Alles in einer Hand, neben dem Tagesgeschäft



int[cube]

Wie Konzerne das lösen: zwei Maschinen

Bewährt, kombinierbar – und sehr teuer

TOP-DOWN

Integriertes Managementsystem (IMS)

Vom Regelwerk über Richtlinien und Rollen zu Prozessen. Beispiel: ISMS & Datenschutz

Regelwerk › Richtlinie › Prozess

BOTTOM-UP

Internes Kontrollsystem (IKS)

Von Kontrollen in den Prozessen über Tests und Belege zu Berichten für Revision und Prüfer.

Kontrolle › Test › Bericht

Beides braucht Tools, Personal, Pflege und Audits. Es lohnt sich erst "at scale".

WAS SICH GERADE ÄNDERT

Mit KI können jetzt auch kleine Organisationen ihre eigenen "Maschinen" bauen!

Am besten keine verkleinerte Kopie von Konzernlösungen.

Der dritte Weg: quer

Vom eigenen Betrieb aus, über alle Regelwerke hinweg

TOP-DOWN

IMS

Vom Regelwerk zum Prozess

BOTTOM-UP

IKS

Von der Kontrolle zum Bericht

QUER

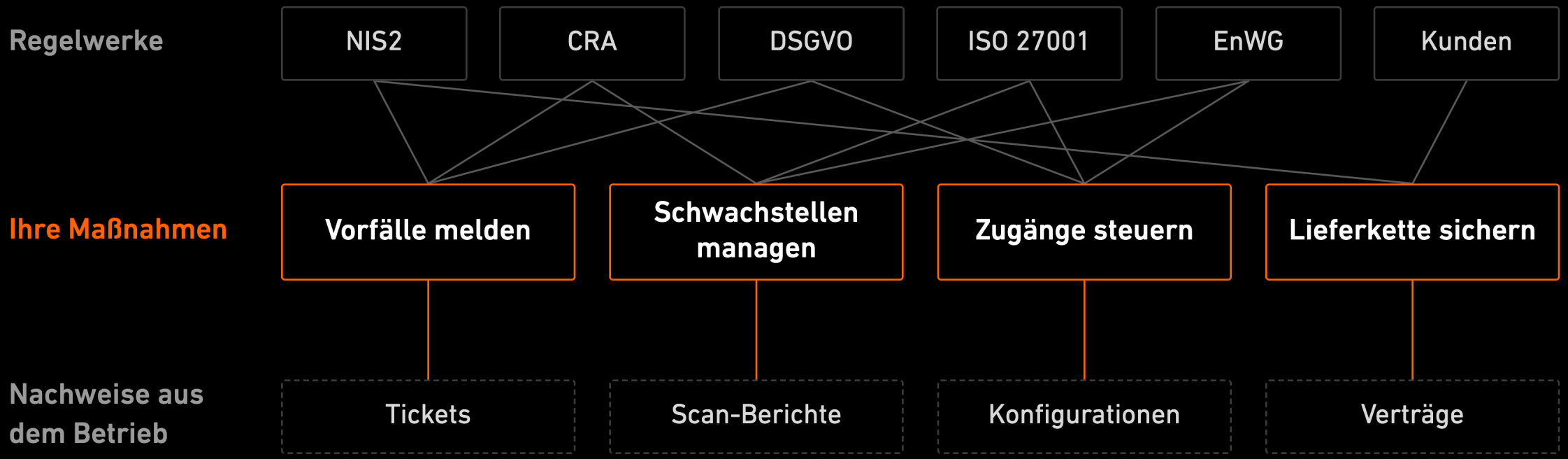
Vom Betrieb aus

KI verbindet, was Sie eh tun,
mit allem, was gefordert ist.

Oben die Regelwerke, unten Ihre Systeme. Die Maschine sitzt in der Mitte:
bei dem, was Sie heute schon tun. Compliance entsteht als "Verdauungsprodukt" nebenher.

Quer gedacht: Ihre Compliance-Landkarte

Einmal tun, vielfach nachweisen



int[cube]

Beispiel: ein Vorfall, ein Ablauf

KI entwirft alle Meldungen

0 h

Vorfall erkannt. Ein interner Ablauf, eine Lagebeschreibung.

24 h

Frühwarnungen für NIS2 und CRA

72 h

Meldungen für NIS2, CRA und DSGVO

Fix + 14 Tage

Abschlussbericht CRA

1 Monat

Abschlussbericht NIS2

Menschen prüfen, entscheiden und senden. KI hilft mit Formularen, Fristen und Abgleich.

int[cube]

Was KI Ihnen nicht abnimmt

Menschen entscheiden.

01

Verantwortung

Die Geschäftsleitung bleibt in der Pflicht, unter NIS2 ausdrücklich.

02

Entscheidungen

Welche Risiken Sie tragen, entscheiden Menschen.

03

Umsetzung

Härten, patchen, üben: Das passiert weiter an Ihren Systemen.

Und: die KI sicher und datenschutzkonform betreiben. (Das wollen Sie aber eh!)

int[cube]

So fangen Sie an

Drei Schritte für die nächsten Wochen

01

Eine Seite: Was gilt für uns?

Regelwerke mit KI auf Ihr Unternehmen eingrenzen und fachlich prüfen.

02

Eine Pflicht durchspielen

Zum Beispiel die Meldewege: einmal von der Anforderung bis zum Nachweis.

03

Nicht allein bauen

In einer Kohorte mit anderen: gleiche Aufgabe, jede ihre eigene Maschine.

int[cube]

Mehr Compliance.
Weniger Aufwand.

Wer baut seine Maschine mit uns?

Scannen oder
einfach ansprechen.

David Fuhr · david@intcube.io
LinkedIn

int[cube]

