

CIS COMPLIANCE SUMMIT 2026 · WIEN

1949, 1971, 2026

Drei Thesen zum Risikomanagement, das
wir haben könnten

Günther Angerbauer
guenther.angerbauer@crisam.net

crisam

1949

1971

2026

Drei Zahlen. Drei Thesen. Und die Behauptung, dass wir in der Informationssicherheit Werkzeuge liegen lassen, mit denen andere Disziplinen längst arbeiten.

Cyber und KI führen das Risk Barometer 2026 an

Allianz Risk Barometer 2026 · Top-Unternehmensrisiken weltweit

01

Cyberverfahren

Betriebsunterbrechung, Datenverlust,
Ransomware

02

Risiken aus dem KI-Einsatz

Neu in der Spitzengruppe, mit der
stärksten Bewegung

Genau diese beiden Risiken
bewerten wir mit den größten
Methoden, die wir haben.

THESE 1

1949

Man kann nicht nicht quantifizieren

Monte Carlo, 1949

Metropolis und Ulam, Los Alamos — benannt nach dem Casino in Monaco

01

Bandbreiten statt Punktwerte

Für Häufigkeit und Auswirkung wird nicht ein Wert geschätzt, sondern ein plausibler Bereich.

02

Tausende Szenarien

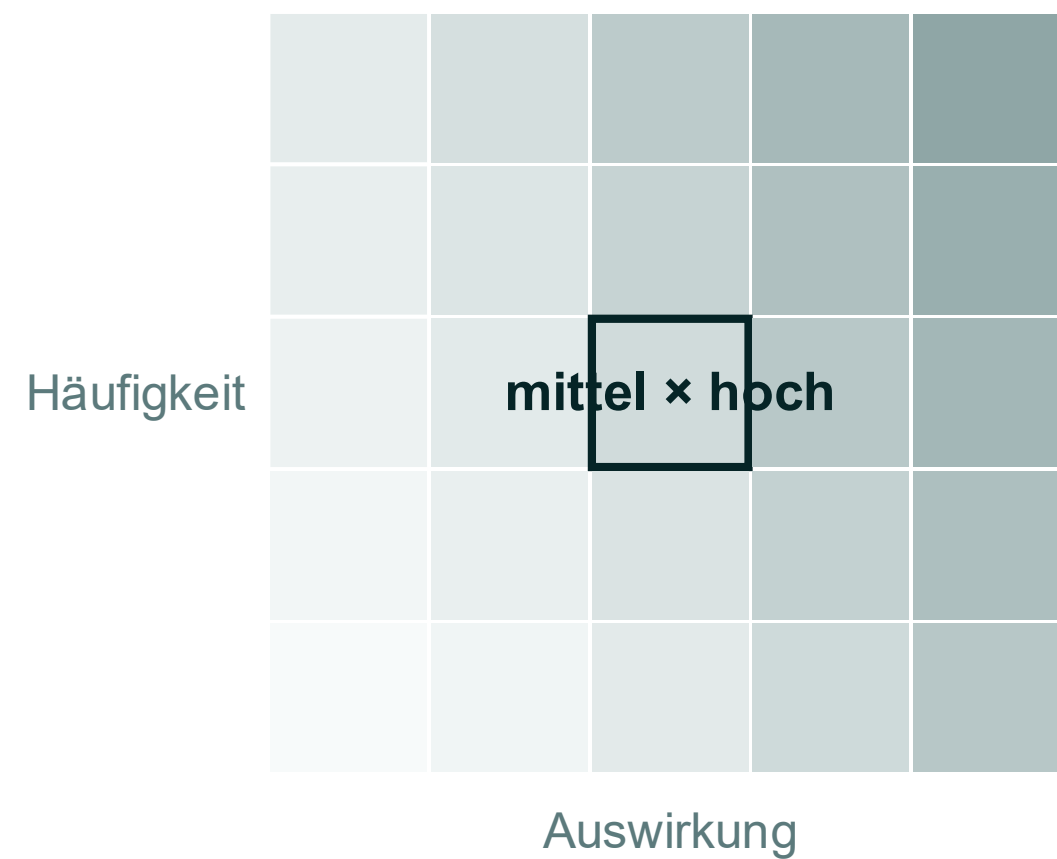
Die Werte werden zufällig gezogen — aber immer innerhalb dieser Bandbreiten.

03

Jedes Szenario ist möglich

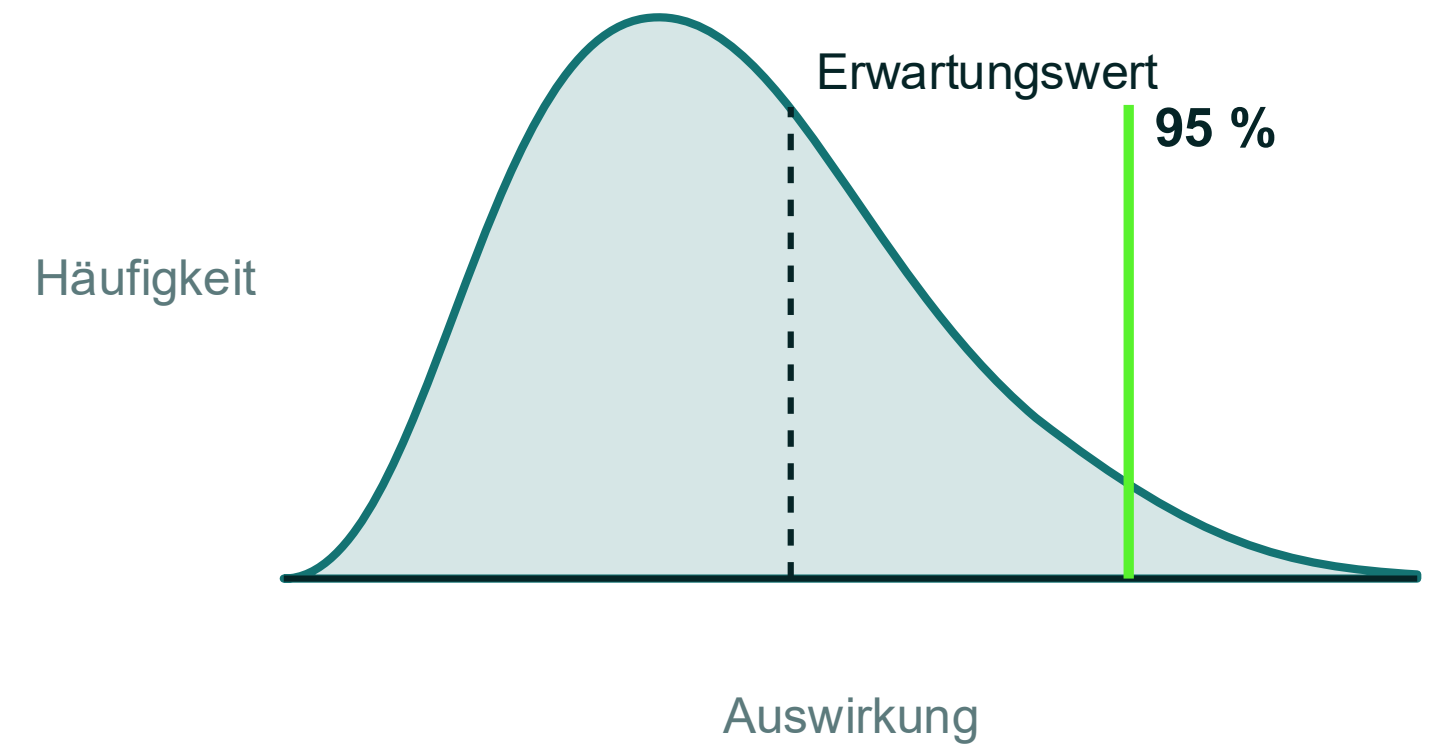
Kein Rechenspiel: jeder einzelne Durchlauf ist ein Verlauf, wie er tatsächlich eintreten könnte.

Matrix und Verteilung im Vergleich



Die Matrix liefert eine Einordnung

Sie sagt nichts über Unsicherheit, lässt sich nicht aggregieren und nicht gegen Budgets rechnen.



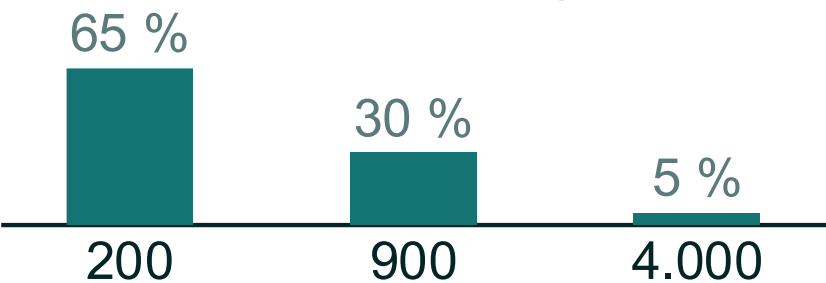
Die Verteilung liefert eine Aussage

Sie zeigt die Unsicherheit, statt sie zu verstecken — und genau deshalb ist sie bei dünner Datenlage die ehrlichere Methode.

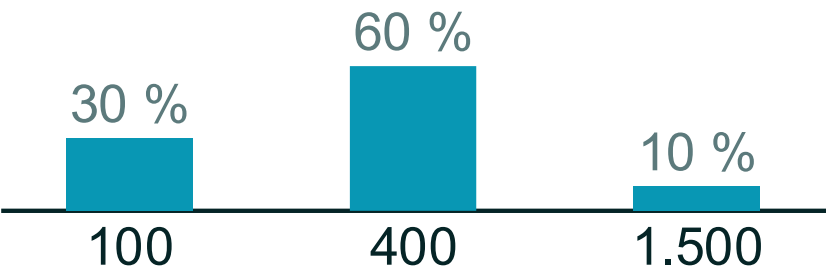
Vom Einzelrisiko zum Gesamtrisiko

Die Simulation zieht alle Risiken gleichzeitig — das Ergebnis ist eine Verteilung, keine Summe · Beispielwerte

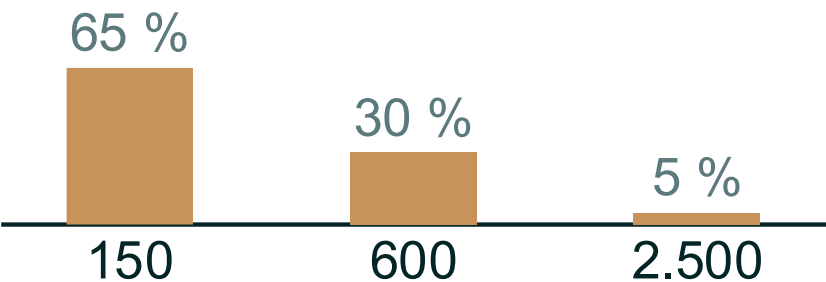
Betriebsunterbrechung · TEUR



Lieferantenausfall · TEUR

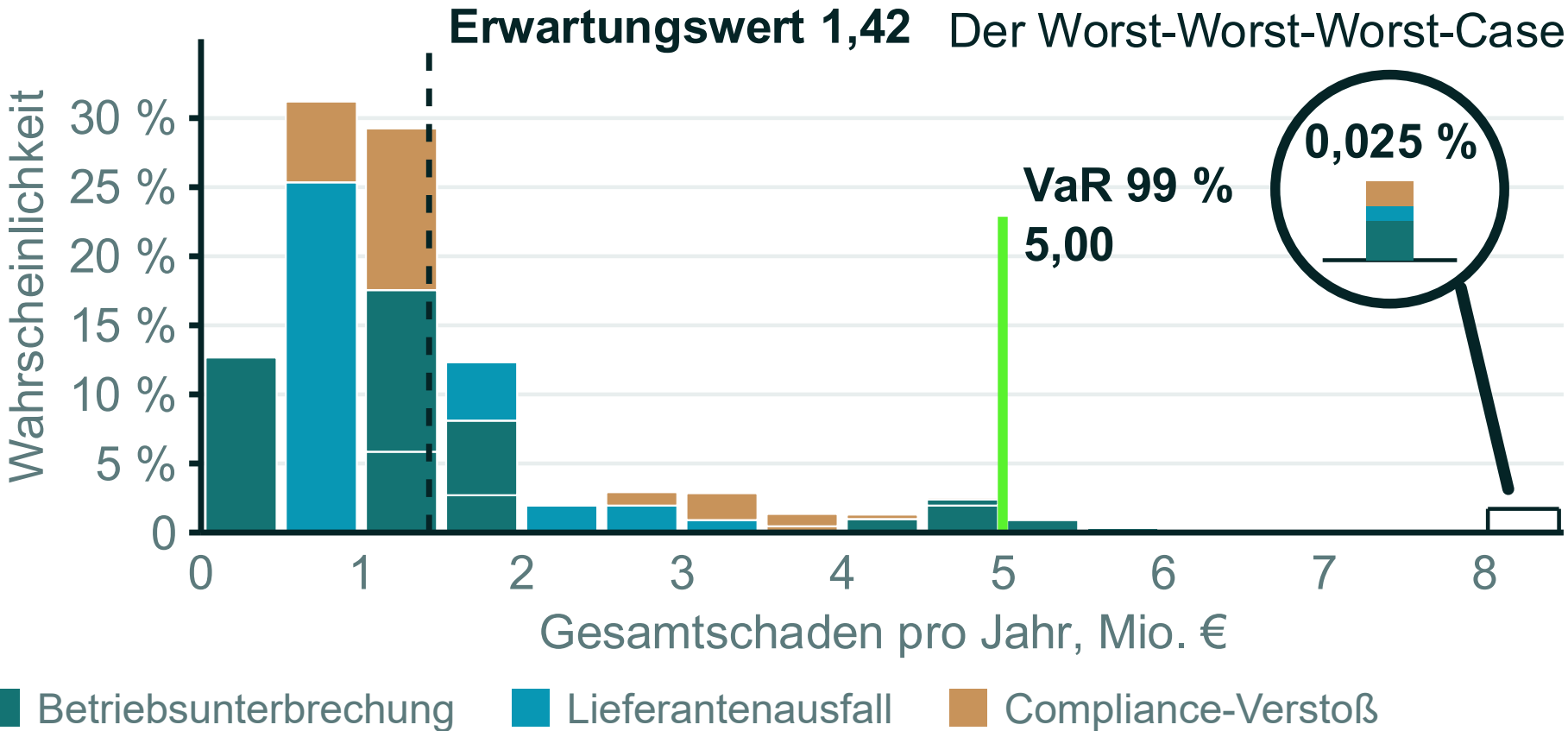


Compliance-Verstoß · TEUR



→
**27
Kombinationen**

Aggregiertes Gesamtrisiko · Klassen von 500 TEUR



Erwartungswert

1,42 Mio. €

VaR 99 %

5,00 Mio. €

Die Addition der Einzel-VaR ergäbe 8,00 Mio. € — **38 % zu viel Risikokapital**, für ein Szenario mit 0,025 % Wahrscheinlichkeit.

Was ein Vorstand hört

MIT DER MATRIX

„Wir haben 30 hohe, 50 mittlere und 30 geringe Risiken.“

Eine Inventarliste. Nicht aggregierbar, nicht vergleichbar, nicht budgetierbar.

MIT VERTEILUNGEN

„Erwartetes Ergebnis 20 Mio. € Gewinn. Das Gesamtrisiko beträgt 5,0 Mio. € — mit 99 % Sicherheit bleiben mindestens 15,0 Mio. €.“

Eine Aussage über das Unternehmen — in derselben Einheit wie jede andere Entscheidung.

THESE 2

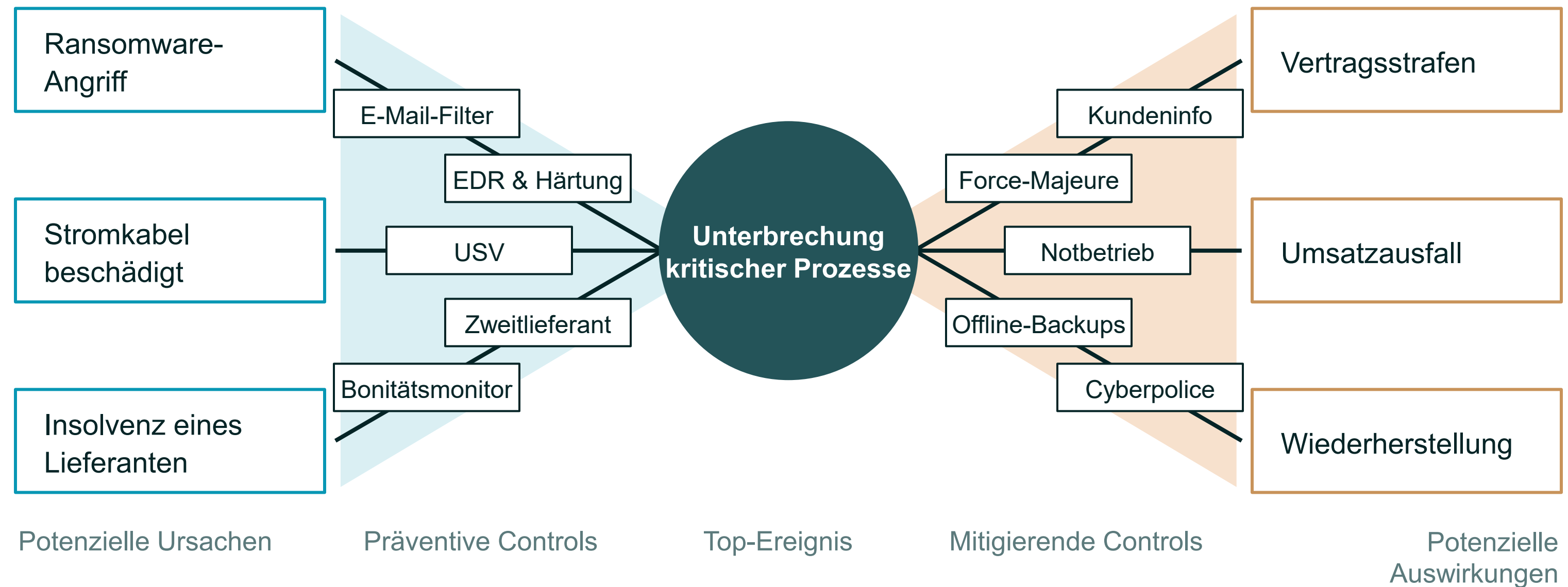
1971

Man kann nicht nicht kommunizieren

Bow-Tie, 1971

Entstanden bei Shell in der Anlagensicherheit

Und ja: benannt ist sie nach dem Mascherl.



Was im Workshop tatsächlich passiert

01

Niemand fragt, wie man das liest.

Fachbereich, IT, Vorstand — die Zeichnung erklärt sich in zehn Sekunden. Ich habe noch keinen Workshop erlebt, in dem ich die Methode erklären musste.

Die Barrieren senken Häufigkeit und Auswirkung — also genau die Verteilungen aus These 1.

02

Die Frage ändert sich.

Aus „ist das jetzt hoch oder mittel“ wird „was fehlt uns links“. Statt zwanzig Minuten über eine Einordnung zu streiten, zeigt jemand auf die Lücke.

03

Wer die Barriere hinzeichnet, diskutiert sie nicht mehr weg.

Der Effekt, der mich am meisten überrascht hat. Maßnahmen, die aus der Zeichnung kommen, muss man später nicht verteidigen.

Die Risikobetrachtung im Grundschutz++ ist entlang des Bow-Tie-Frameworks aufgebaut — Risikoszenarien links, Verlust eines Schutzziels in der Mitte, Auswirkungen rechts.

Die Beispielmethoden sind ausdrücklich nicht verpflichtend. Aber der BSI-Standard 200-3 wird eingestellt — und im Nachfolger ist die Bow-Tie-Methode die tragende Struktur.

THESE 3

2026

Man kann nicht nicht delegieren

AI verändert alles - auch im Risikomanagement

●

2020

Echtzeiterkennung

Web-Crawler, News-Clustering, Sentimentanalyse, Scheduler. Stand der Technik: Transformer, die Sätze vervollständigen.

●

2022

LLMs

LLMs können Beschreibungen verbessern. Assistenten können allgemeine Fragen beantworten.

●

2026

Bewertung durch ein Gremium

Verteilungen für Häufigkeit und Auswirkung, hergeleitet und nachvollziehbar — genau das, was als unmöglich galt.

Anwendungsfall 1: Risikoquantifizierung

Ransomware-Risiko, bewertet von einem Gremium mehrerer KI-Analysten — akkreditierte Zertifizierungsstelle, 13 Mitarbeitende, 4,2 Mio. € Umsatz

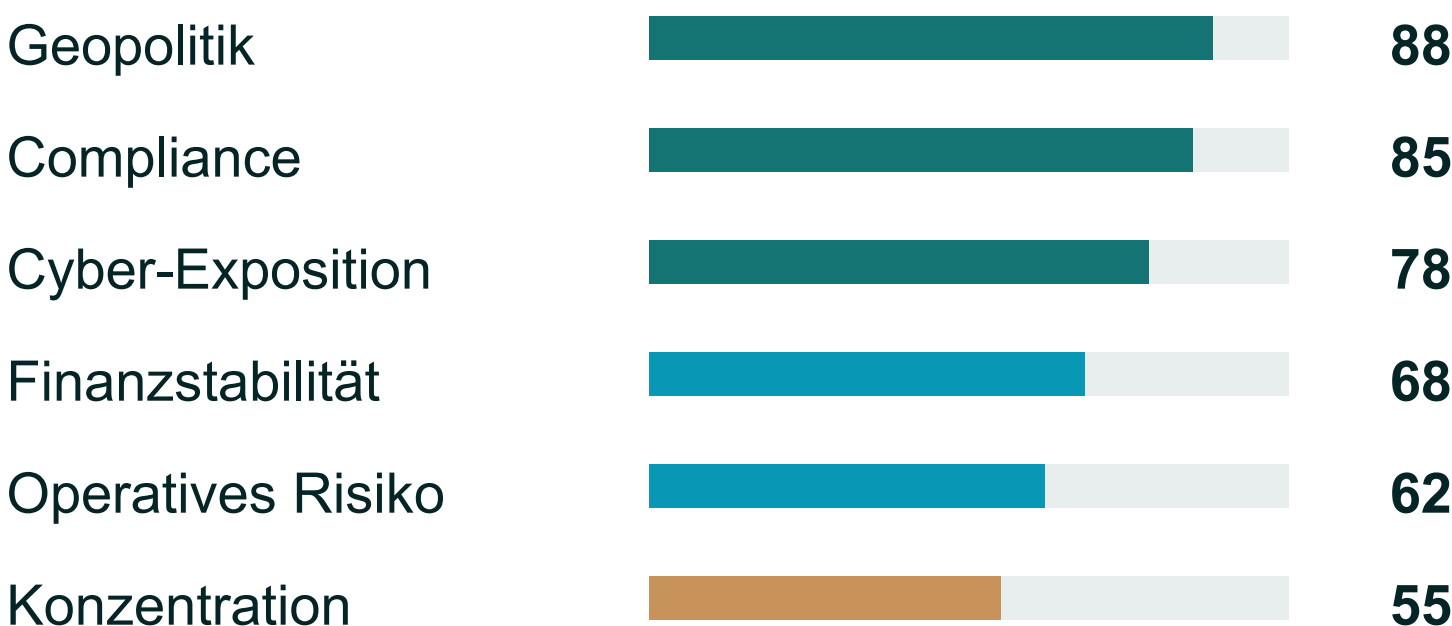
MODELL	ERGEBNIS		MITGELIEFERT
Häufigkeit: Poisson $\lambda = 0,15$ — drei materielle Ereignisse in zwanzig Jahren, also 13,9 % Wahrscheinlichkeit pro Geschäftsjahr.	Erwartungswert	Standardabweichung	Begründung der Verteilungswahl — Poisson gegen Binomial, mit Ableitung
	243.500 €	729.300 €	Kalibrierung an Benchmarks: Sophos, Verizon DBIR, ENISA, IBM/Ponemon
Auswirkung: PERT 150 T€ Minimum, 900 T€ Modalwert, 6,0 Mio. € Maximum, $\lambda = 4$.	VaR 99 %	Expected Shortfall	Rechenweg in sieben Schritten, analytisch gegengeprüft
	3,52 Mio. €	4,27 Mio. €	Konvergenzprüfung über drei Teilstichproben
			Eigene Modellkritik: Bandbreite $\lambda = 0,08$ bis 0,25 offen ausgewiesen

Der VaR 99 % entspricht dem 2,2-Fachen des Eigenkapitals — die Aussage, die aus einer Ampelfarbe nie herauszulesen wäre.

Anwendungsfall 2: Lieferantenrisikobewertung

Dasselbe Gremium, öffentliche Quellen, sechs Dimensionen — jede Bewertung mit Begründung und Quelle

73 von 100 · Gesamtbewertung „medium“



BEGRÜNDUNG ZUR SCHWÄCHSTEN DIMENSION

„Die Umsatzbasis ist auf ein Marktsegment und einen Abnehmerkreis konzentriert; beide reagieren auf denselben regulatorischen Auslöser. Der hohe Marktanteil stützt die Bewertung, reduziert die Konzentration aber nicht.“

Sechs Nachrichtensignale mit Datum, Bewertung und Quelle

Sieben Kernrisiken und acht Mitigationen, jeweils im Volltext

Explizite Flags dort, wo keine Evidenz gefunden wurde

1949

Man kann nicht nicht quantifizieren

1971

Man kann nicht nicht kommunizieren

2026

Man kann nicht nicht delegieren

Alle drei machen Ihr Risikomanagement besser — und mit jeder einzelnen können Sie morgen anfangen.



Günther Angerbauer

guenther.angerbauer@crisam.net

+43 664 2127457

crisam