



**Technische Hochschule
Brandenburg**
University of
Applied Sciences
**Fachbereich
Wirtschaft**

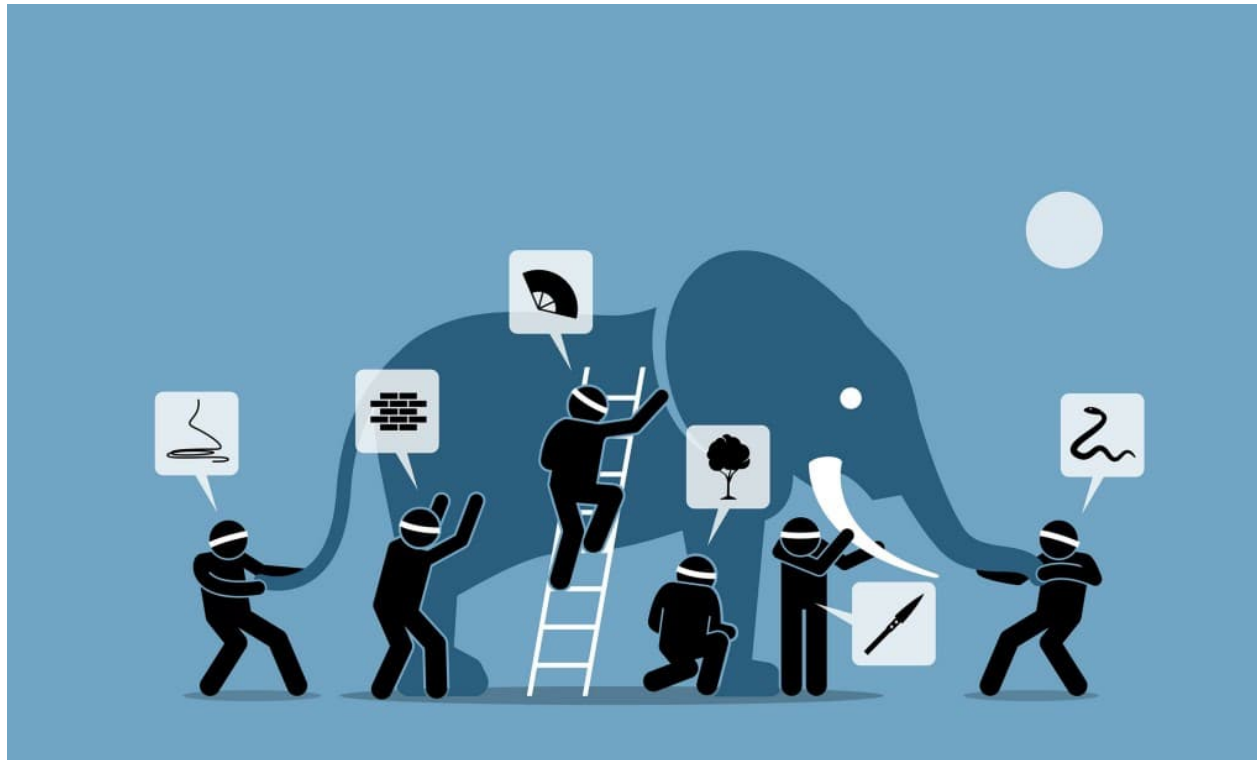
Security Governance als Führungsaufgabe – für Konzerne, Mittelstand und Kleinunternehmen

18. Security Forum der Technischen Hochschule Brandenburg, 15.01.2026





Haben Sie in Ihrem Unternehmen oder in Ihrer Institution eine integrierte Sicht auf Sicherheit – oder sehen Sie einzelne Teile wie die blinden Männer bei dem Elefanten?



Security Governance sorgt dafür, dass aus Fragmenten ein ganzheitliches Sicherheitskonzept wird.



Security Governance als Führungsaufgabe



- Verantwortung liegt bei Vorstand & Geschäftsführung
- Tone from the Top prägt die Sicherheitskultur
- Klare Entscheidungsprozesse für Transparenz und Risikoakzeptanz
- Strategische Integration externer Vorgaben



Architektur: Security Governance – Prozesse – Risiko



Security Governance-Ebene

Security Governance definiert strategische Sicherheitsziele, Verantwortlichkeiten und den Risk Appetite.

Prozessebene und ISMS

Security Prozesse übersetzen Governance in operative Maßnahmen wie ACP, Incident- und Continuity-Management. Geschäftsprozesse schaffen Transparenz über Vermögensgüter.

Risikomanagement

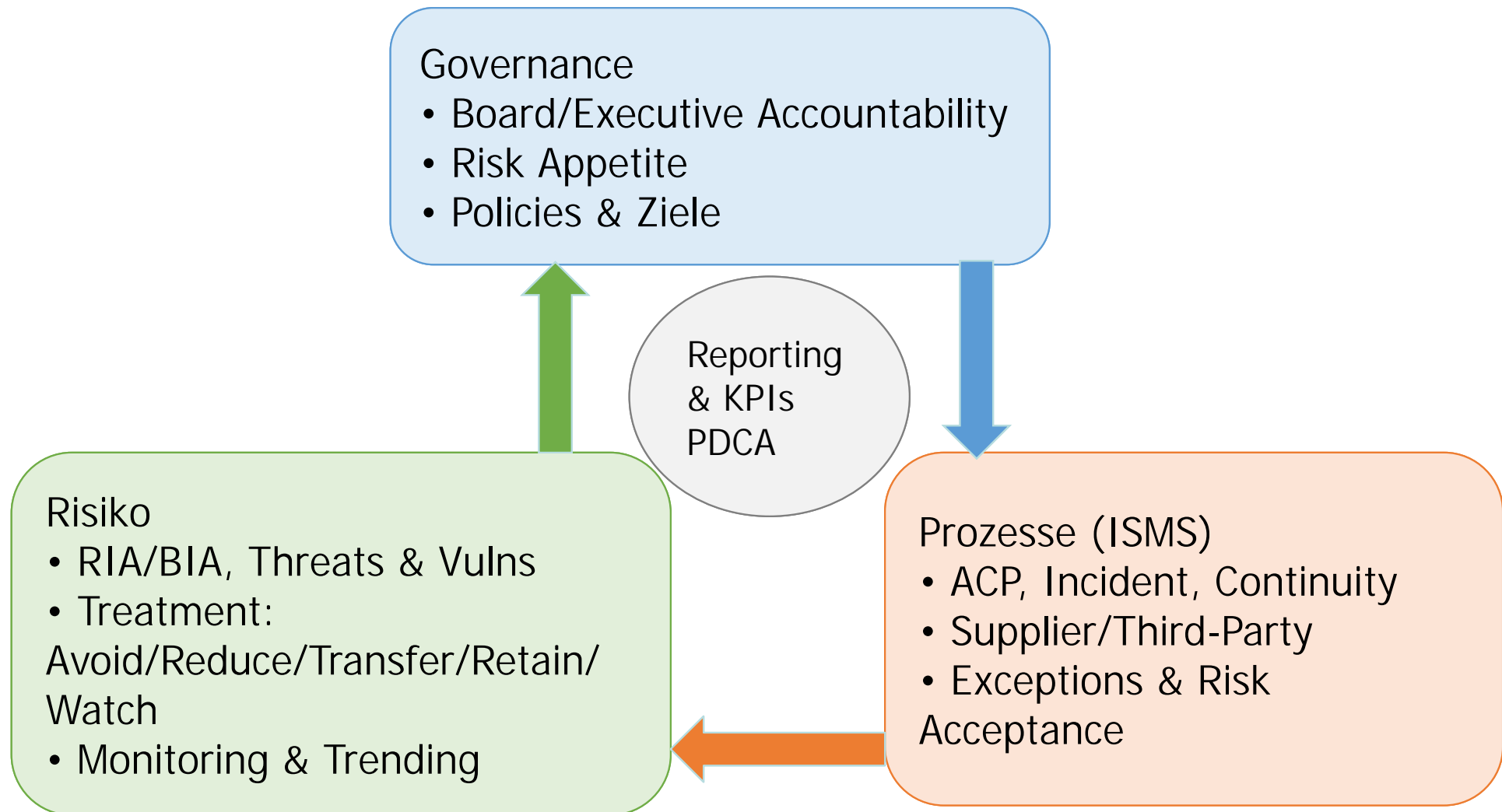
Risikomanagement nutzt RIA und BIA und priorisiert und legitimiert Entscheidungen.

Kontinuierliche Verbesserung

Reporting und PDCA steuern.



Zusammenhang: Governance – Prozesse – Risiko



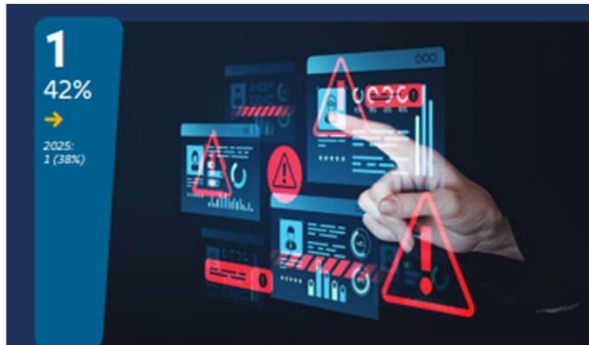
Kontext: Business-Strategie, Regulierung (z. B. NIS2, CRA), Geopolitik

Quelle: Saatmann, 2026

Wie ist die Lage?



Allianz Risk Barometer 2026



Cyber incidents

(e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)



Artificial intelligence

(e.g., implementation challenges, liability exposures, misinformation / disinformation)



Business interruption

(incl. supply chain disruption)



Changes in legislation and regulation

(e.g., tariffs, new directives, sustainability requirements)



Natural catastrophes

(e.g., storm, flood, earthquake, wildfire)



Climate change

(e.g., physical, operational and financial risks as a result of extreme weather)



Political risks and violence

(e.g., war, political instability, terrorism, polarization, coup d'état, civil unrest, strikes, riots, looting)



Macroeconomic developments

(e.g., inflation, deflation, monetary policies, austerity programs)



Fire, explosion¹



Market developments

(e.g., intensified competition / new entrants, M&A, market stagnation, market fluctuation)

Key

↑ Risk higher than in 2025
↓ Risk lower than in 2025

→ No change from 2025
(5%) 2025 risk ranking %

¹ Fire, explosion ranks higher than market developments based on the actual number of responses

² Critical infrastructure blackouts ranks higher than talent or labor issues based on the actual number of responses

³ Theft, fraud, corruption ranks higher than insolvency based on the actual number of responses

⁴ Loss of reputation or brand value ranks higher than biodiversity and nature risks based on the actual number of responses

⁵ Biodiversity and nature risks ranks higher than product recall, quality management, serial defects based on the actual number of responses

The most important global business risks for 2026

Ranking changes are determined by positions year-on-year, ahead of percentages.

The 15th annual **Allianz Risk Barometer** survey was conducted among Allianz customers (global businesses), brokers and industry trade organizations. It also surveyed risk consultants, underwriters, senior managers and claims experts in the corporate insurance segment of Allianz Commercial and other Allianz entities.

[View the full Allianz Risk Barometer 2026 rankings here](#)

Rank		Percent	2025 rank	Trend
11	Critical infrastructure blackouts (e.g., power disruption) or failures (e.g., aging dams, bridges, rail tracks) ²	8%	12 (9%)	↑
12	Talent or labor issues	8%	11 (9%)	↔
13	Energy crisis (e.g., supply shortage / outage, price fluctuations)	6%	13 (8%)	→
14	Theft, fraud, corruption ³	5%	14 (7%)	→
15	Insolvency	5%	16 (6%)	↑
16	Loss of reputation or brand value (e.g., public criticism) ⁴	4%	15 (7%)	↔
17	Biodiversity and nature risks (e.g., water scarcity) ⁵	4%	NEW	↑
18	Product recall, quality management, serial defects	4%	18 (4%)	→
19	Human health risk (e.g., pandemic outbreak)	3%	19 (3%)	→
20	Pollution event	1%	17 (6%)	↔
	Other	2%		

Source: Allianz Commercial

Figures represent the number of risks selected as a percentage of all survey responses from 3,338 respondents. All respondents could select up to three risks per industry, which is why the figures do not add up to 100%.

NEW New entry in the top risks

Quelle: Allianz, 2026



Allianz Risk Barometer 2026



- Cyber incidents is the top global risk for 2026 – 10% ahead of AI
- Cyber incidents ranks #1 the fifth year in a row. A decade ago, it ranked only #8.
- It is the top risk across all company sizes (large, mid-sized and small).

Quelle: Allianz, 2026



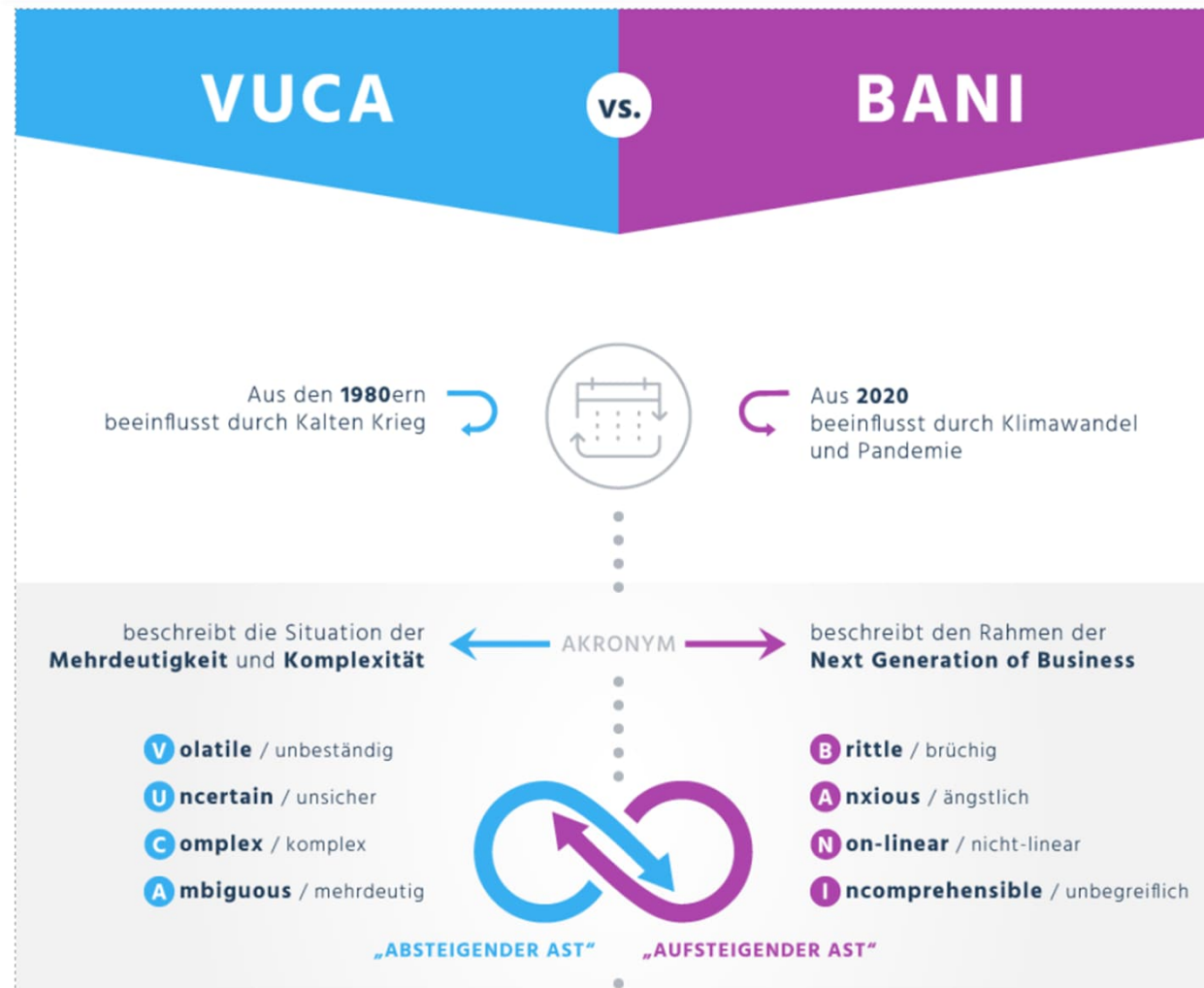
Der sicherheitspolitische Start ins neue Jahr 2026.





Frameworks helfen als Grundannahme der Security Governance

VUCA- wird zur BANI-Welt



<https://www.resilienz-akademie.com>



VUCA-Welt wird zur BANI-Welt



<https://www.resilienz-akademie.com>



Technische Hochschule

Brandenburg

University of
Applied Sciences

**Fachbereich
Wirtschaft**

Wie erfolgt die Umsetzung in Unternehmen?



Security Governance als Führungsaufgabe – Überblick über die Umsetzung

<u>Aspekt</u>	<u>Konzerne</u>	<u>Mittelstand</u>	<u>Kleinunternehmen</u>
Strategische Ebene	Vorstandsebene, CISO, Governance Board	Geschäftsführung + IT-Leitung	Inhaber oder externe IT-Dienstleister
Führungsrahmen /Standards	ISO/IEC 27014, NIST CSF, COBIT	ISO/IEC 27001 (vereinfachte Umsetzung), BSI IT-Grundschutz	BSI Basisabsicherung, ENISA SME Guidelines
Rollen & Verantwortl.	Klare Rollen: CISO, Risk Officer, Compliance	Wenige Rollen, oft kombiniert (IT + Security)	Meist keine dedizierte Rolle, „One-Man-Show“
Prozesse	Formelle Governance-Prozesse, KPIs, Audits	Teilweise formalisiert, oft projektbezogen	Ad-hoc, stark abhängig von Awareness
Budget & Ressourcen	Hohe Budgets, dedizierte Teams	Begrenzte Budgets, externe Beratung	Minimal, Fokus auf kostengünstige Lösungen
Risikoansatz	Risikomanagement integriert in Unternehmensstrategie	Risikoanalyse punktuell, oft reaktiv	Fokus auf Basis-Schutz, kaum strategisch

Quelle: Saatmann, 2026



Cybersecurity im Mittelstand – Lage 2025

80 % aller gemeldeten Vorfälle betreffen KMU (BSI-Lagebericht 2025)

KMU sehen Cybersecurity als größte Herausforderung – vor Energiepreisen und Bürokratie (it-sa Barometer)

Hauptprobleme:

- Veraltete Systeme, fehlende Backups
- Mangelnde Awareness & fehlende Notfallpläne
- IT-Sicherheit oft nicht strategisch verankert

Bedrohungen: Phishing, Malware, gestohlene Zugangsdaten, Lieferkettenangriffe

Folgen: Hohe Schadenssummen, Insolvenzrisiko bei fehlendem Business Continuity Management

Handlungsbedarf:

- Regelmäßige Updates & Schulungen
- Backup-Strategie & Notfallpläne
- Nutzung von BSI-Leitfäden & Förderprogrammen
- Resilienz umfasst Prävention, Verteidigung und Bewältigung
- Cyberrisiko-Check des BSI



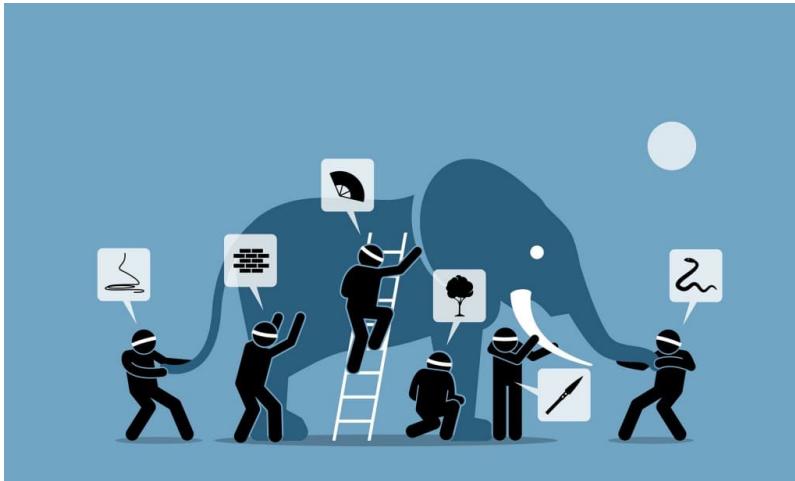
Quelle: BSI, 2025



Governance entscheidet – Prozesse setzen um – Risiko priorisiert Diskutieren Sie mit uns – Wie verankern Sie Security Governance in ihrem Unternehmen?

Security Governance als Steuerungshebel

Security Governance definiert strategische Steuerung und
Verantwortlichkeit für wirksame Informationssicherheit.



Klare Entscheidungsrechte

Unklare Verantwortlichkeiten führen zu ineffizienten
Prozessen und Sicherheitsvorfällen trotz technischer
Investitionen.

Security Governance als Führungsaufgabe

Security Governance ist keine IT-Aufgabe, sondern ein
Führungsprozess, der Sicherheitsziele in der
Unternehmensstrategie verankert.

Konfliktlösung und Resilienz

Security Governance ermöglicht strategische Lösung von
Zielkonflikten und stärkt die Organisation gegen
Bedrohungen.

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Stefan Saatmann
(Lehrbeauftragter an der THB seit WS 2020)

stefan.saatmann@th-brandenburg.de

Technische Hochschule Brandenburg
University of Applied Sciences
Fachbereich Wirtschaft
Magdeburger Straße 50
14770 Brandenburg an der Havel

www.th-brandenburg.de/wirtschaft

