



3. IT-Grundschutz-Tag 2023

Informationssicherheit als Motor organisationaler Resilienz

Unser **Unternehmenssitz**

Tradition trifft **Hightech**

- Im **denkmalgeschützten** Walderdorffer Hof in **Limburg an der Lahn**
- **Ideale Anbindung** (Bahn, Flug, PKW) im Drehkreuz zwischen Frankfurt am Main und Köln



Exzellente in der Informationssicherheit

- Von der **Gap-Analyse** bis zum vollständigen ISMS
- ISO/IEC 27001 oder BSI IT-Grundschutz



- **Asset Management**,
- **Informationssicherheit**,
- **Risikomanagement**
- **Information Security Controlling** etc.

- **Zusammenführung** der Managementsysteme für Informationssicherheit, IT-Services, Business Continuity und Datenschutz

- **Interne Audits** und Assessments

- **Chief Information Security Officer as a Service (CISOaaS)**
- **Aus- und Weiterbildung** mit **CARMAO Academy for organizational Resilience**

Anspruchsvolle BCM/IT-SCM-Lösungen

- Business Continuity und IT-Service Continuity Management
- ISO/IEC 22301 oder BSI 100-4 bzw 200-4.



- Von der Business Impact Analyse bis zum vollständigen BCMS
- Zertifizierungsvorbereitung nach ISO/IEC 22301

- Vom Notfallmanagement bis zur Krisenstabsübung
- Business Continuity Manager und Business Risk Manager as a Service (BCMaaS/BRMaaS)

- Audits und Assessments

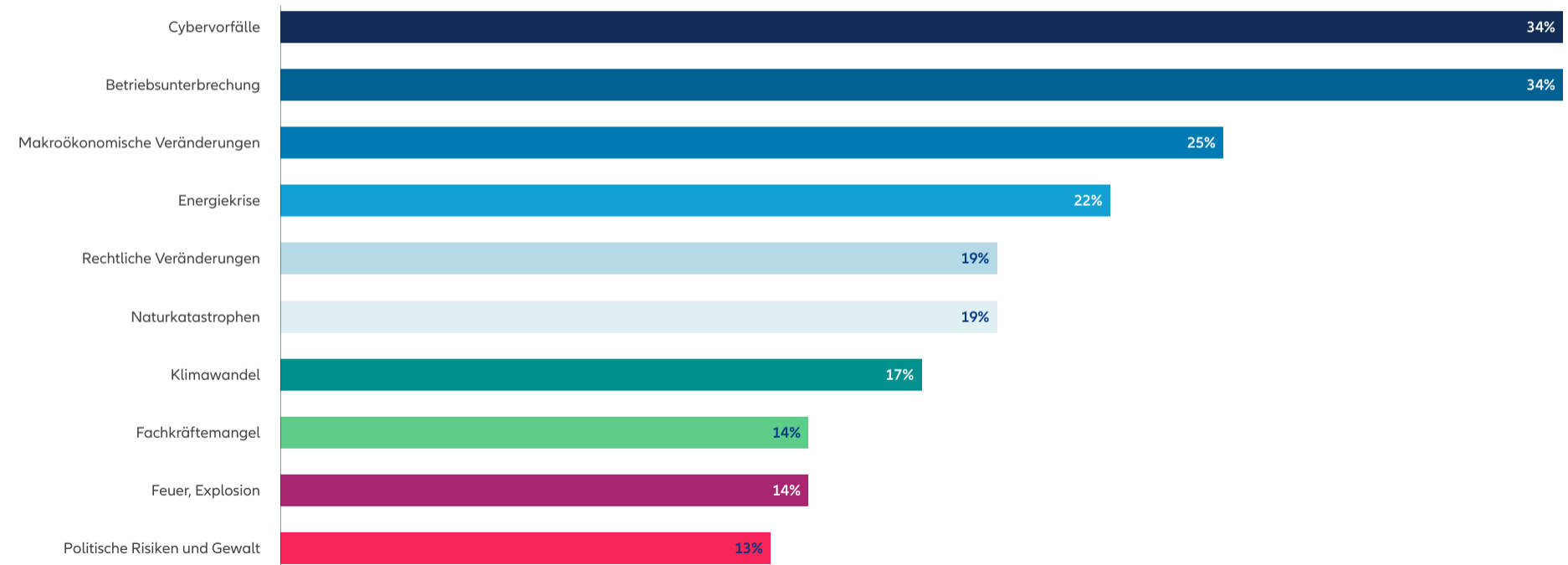
- Aus- und Weiterbildung mit CARMAO Academy for organizational Resilience



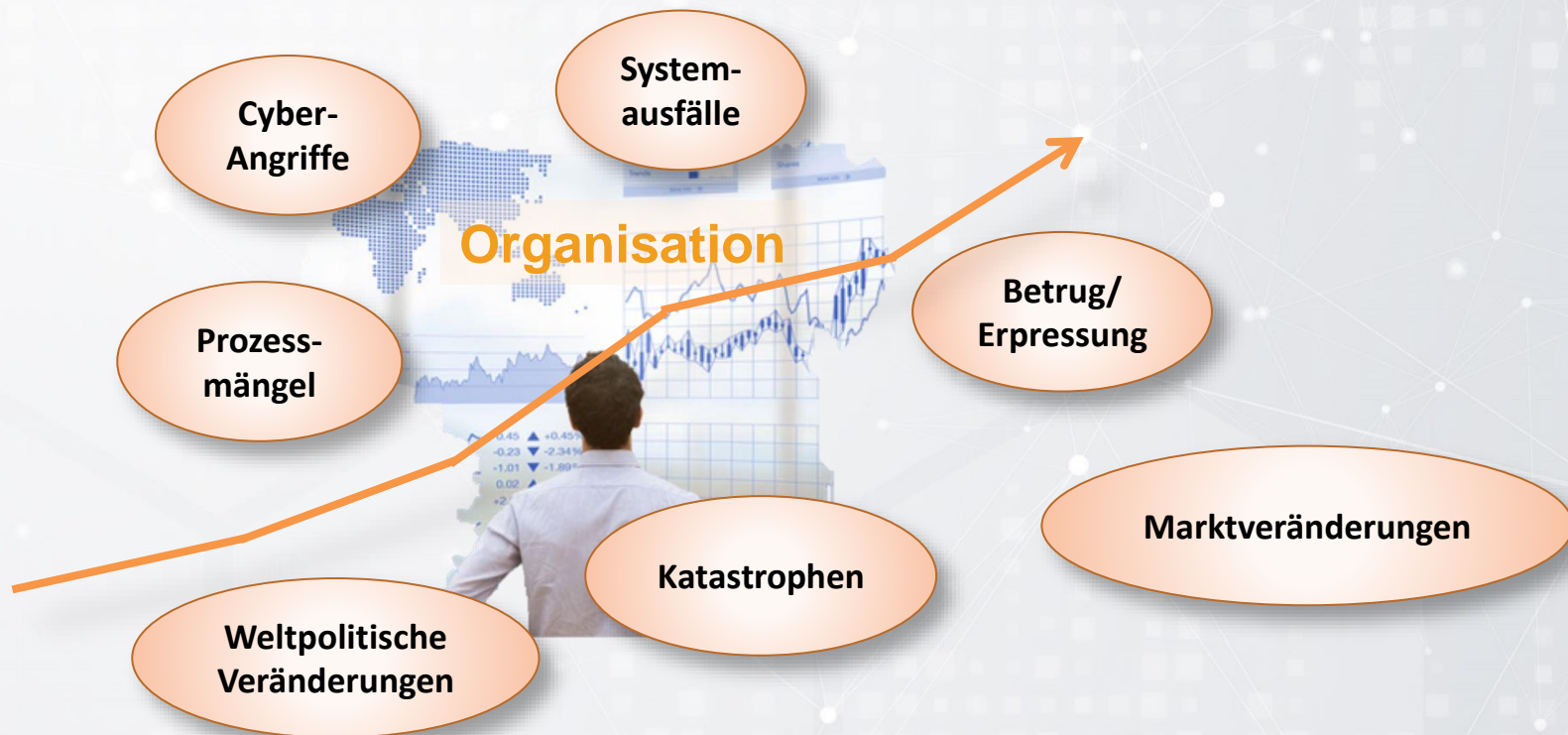
Top 10 Geschäftsrisiken weltweit in 2023

Allianz Risk Barometer 2023

Basierend auf den Antworten von 2.712 Risikomanagement-Experten aus 94 Ländern und Gebieten (% der Antworten). Die Zahlen ergeben nicht 100%, da jeweils bis zu drei Risiken ausgewählt werden konnten.



Organisationen sind vielfältigen **Gefahren** ausgesetzt ...



... und benötigen eine **widerstandsfähige** bzw. eine **resiliente** Organisation

Was bedeutet **organisationale Resilienz**?

Organisationale Resilienz ist die Fähigkeit einer Organisation, etwas abzufedern und sich in einer verändernden Umgebung anzupassen, um so ihre Ziele zu erreichen, zu überleben und zu gedeihen.

Resilientere Organisationen können Risiken und Chancen – aufgrund von plötzlichen oder allmählichen Veränderungen im internen und externen Kontext – antizipieren und darauf reagieren.

Attribute einer **resilienten Organisation**

Die Organisation im Spannungsfeld zwischen Sicherheit und Flexibilität:

- **Flexible** Organisation
 - Agile Prozesse und Organisationsformen, Führung
- **Geschützte** Organisation
 - Präventiver Schutz der Prozesse, Organisation, Infrastruktur, Personen
- **Robuste** Organisation
 - Etabliertes Notfall- und Disaster Recovery-Management
- **Kompetente** Organisation
 - Aktive Personalentwicklung, Training- und Awareness-Programme
- **Antifragile*** Organisation
 - Ausbildung von positiven Veränderungen wegen und während einer Krise

* Anti-Fragilität – Anleitung für eine Welt, die wir nicht verstehen von Nassim Nicholas Taleb, 2012

Relevante Managementdisziplinen nach ISO 22316

Asset Management

Crisis Management

Fraud Control

Business Continuity Management

Risk Management

Supply Chain Management

Communications Management

Emergency Management

Quality Management

Cyber Security Management

Human Resources Management

Financial Control

Facilities Management

Information Security Management

Governance

Strategic Planning

Environmental Management

Physical Security Management

Information, Communications and Technology

Health and Safety Management

Einfluß der **Informationssicherheit**

- **Flexible** Organisation
 - Verpflichtung der Organisationsleitung, Zuordnung von Rollen und Verantwortlichkeiten, Risikomanagement, dokumentierte und regelmäßig überprüfte Prozesse
- **Geschützte** Organisation
 - Ermittlung Schutzbedarf, Risikobehandlung, Festlegung und Umsetzung von organisationspezifischen Sicherheitsanforderungen, Betrieb eines SOC
- **Robuste** Organisation
 - Aufbauend auf einem Security Incident Management Framework
- **Kompetente** Organisation
 - Entwicklung der Führungskräfte, Security Training und Mitarbeiter-Awareness-Programme
- **Antifragile*** Organisation
 - Monitoring, Reviews, Identifizierung von Korrekturmaßnahmen, kontinuierliche Verbesserung,

Das Zusammenspiel aus den IT Grundschutz-Dokumenten 200-1 bis 200-4 zusammen mit dem Grundschutz-Kompendium bieten eine passende Grundlage.

Keine Resilienz ohne tiefes Wissen zur Organisation

- Wer die Organisation nicht ausreichend kennt, kann nicht im Sinne und zum Wohle der Organisation handeln
 - Internes und externes Umfeld der Organisation
 - Ziele der Organisation
 - Informationsverbund
 - Schutzbedarf
 - Risikoszenarien
 - Kontinuierlich an Veränderungen anpassen!!!

Ausflug: Anti-Fragilität einer Organisation

- Verbindung von Sicherheit, Kreativität und Flexibilität
- Lernen und Weiterentwickeln in der Krise (Bspw. Pandemie)
 - Siegeszug der Online-/Videokommunikation und virtuellen Zusammenarbeit
 - Wegfall ganzer Geschäftsmodelle und kurzfristiger Um- und Aufbau neuer Aktivitäten (Vom Eventmanager zum CORONA-Testbetreiber, etc.).

Förderung offenen Miteinanders

Schaffung kreativer Zeit(-modelle)

Förderung von Querdenken

Experimentieren und Ausprobieren



Vielen Dank für Ihre Aufmerksamkeit

Organisationale Resilienz im Überblick:

- **Flexible** Organisation
 - Agile Prozesse und Organisationsformen, Führung
- **Geschützte** Organisation
 - Präventiver Schutz der Prozesse, Organisation, Infrastruktur, Personen
- **Robuste** Organisation
 - Etabliertes Notfall- und Disaster Recovery-Management
- **Kompetente** Organisation
 - Aktive Personalentwicklung, Training- und Awareness-Programme
- **Antifragile*** Organisation
 - Ausbildung von positiven Veränderungen wegen und während einer Krise

* Anti-Fragilität – Anleitung für eine Welt, die wir nicht verstehen von Nassim Nicholas Taleb, 2012

Sie haben noch Fragen?

Sprechen Sie mich gerne an.

Ulrich HEUN

Geschäftsführender Gesellschafter

Telefon: +49 6431 2196-0

E-Mail: ulrich.heun@carmao.de

CARMAO GmbH | Walderdorffer Hof | Fahrgasse 5 | 65549 Limburg