Was hat organisationale Resilienz mit IT-Grundschutz zu tun?

BSI-IT-Grundschutz-Tag

Olaf Jüptner, Enterprise Europe Network Hessen, Hessen Trade & Invest GmbH

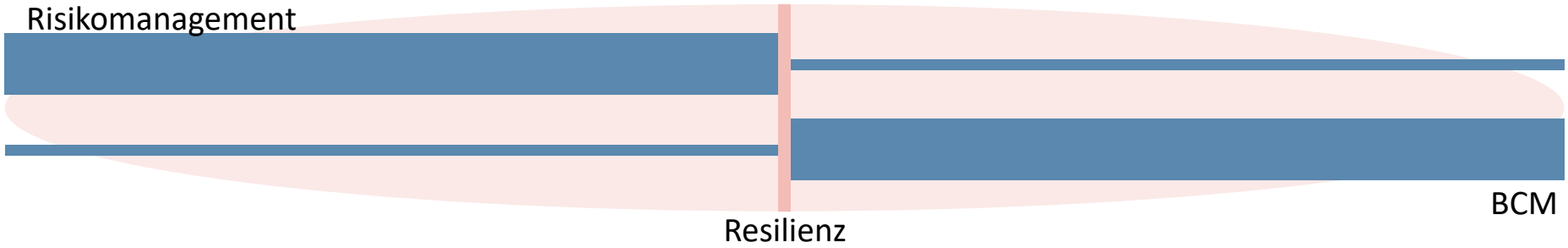
HESSEN

Hessisches Ministerium
für Wirtschaft, Energie,
Verkehr und Wohnen

Was ist organisationale Resilienz?

"Resilienz ist die Fähigkeit, Veränderungen in der Umgebung aufzunehmen und sich an diese anzupassen" (ISO 22300)

- Thesaurus u.a.: Robustheit, Selbstregulation, Standhaftigkeit, **Widerstandsfähigkeit**, Widerstandskraft, Zähigkeit (wiktionary)
- Resiliente Unternehmen können **Chancen und Bedrohungen** sowohl aus plötzlichen als auch aus graduellen internen und externen Veränderungen erkennen und darauf reagieren. (ISO 22316)
- **Resilienz als Fähigkeit, Zustand:** Resilienz wird erreicht durch systematisches Nutzen mehrerer Tools und Methoden, zentral ist u.a. das Risikomanagement.



World Trade Center, 9/11, 8:47 Uhr

- Morgan Stanley
- 2700 Angestellte im Südturm
- 8:46 Uhr: erstes Flugzeug im Nordturm
- 8:47 Uhr: Evakuierungsbeginn MS im Südturm
- Grund: nach WTC-Attentat 1993 Aktionsplan mit regelmäßigen Übungen; Sicherheitschef mit Megaphon; nur 7 Tote
- MS nahm die Arbeit am Folgetag an drei Notstandorten auf

Die Normenwelt der Resilienz

"Resilienz ist die Fähigkeit, Veränderungen in der Umgebung aufzunehmen und sich an diese anzupassen" (ISO 22300)

Auswahl:

- **ISO 22316** Security and resilience — **Organizational resilience**
- **ISO 22301** Security and resilience — **Business continuity** management systems — Requirements (A)
- **ISO 27001** Information security, cybersecurity and privacy protection — **Information security management systems** — Requirements (A)
- **ISO 28002** Security management systems for the supply chain — **Development of resilience in the supply chain** — Requirements with guidance for use (A)
- **ISO 31000 Risk management** — Guidelines
- **ISO 37001 Anti-bribery** management systems — Requirements with guidance for use (A)
- **ISO 37301 Compliance** management systems (A)
- **ISO/CD 56001 Innovation management -** Innovation management system – Requirements (A)

(A): zertifizierbarer Standard

Organisationale Resilienz

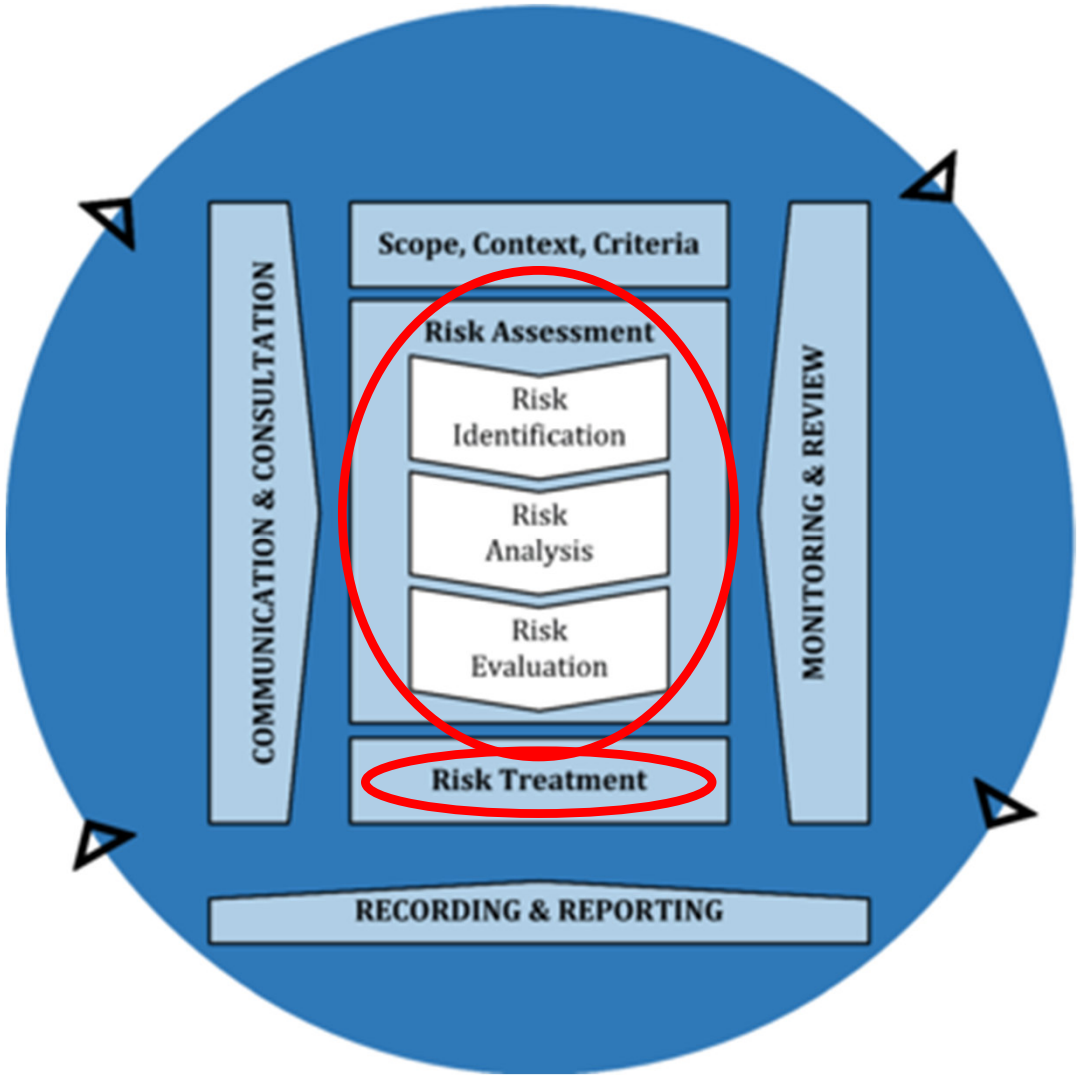
Nach **ISO 22316**: Sicherheit und Resilienz – Organisationale Resilienz – Grundsätze und Merkmale

Merkmale	**Management-Disziplinen** (Anhang A; ausgewählte)
Geteilte Vision und klares Ziel	Business-Continuity-Management
Umfeld verstehen und beeinflussen	Krisenmanagement
Effektive und ermutigende Führung	Cybersicherheitsmanagement
Resilienzfördernde Kultur *	Kommunikationsmanagement
Information und Wissen teilen	Umweltmanagement
Verfügbarkeit von Ressourcen	Governance
Koordinierte Unternehmensbereiche	Finanzmanagement
Kontinuierliche Verbesserung fördern	Informationssicherheit
Antizipation von Veränderungen	Lieferkettenmanagement
	Strategische Planung

* Ein Element ist eine agile, flexible, kompetenzorientierte Einstellung sowie eine positive Fehlerkultur.

Risikomanagement-Prozess

(ISO 31000)



IEC 31010: Risk management — **Risk assessment techniques**

Vergleich Risikomanagement ISO-BSI

ISO 31000:2018

- **Kontextbeschreibung**
- **Risikoidentifikation**
  (kreativer Prozess mithilfe von Verfahren)
- **Risikoanalyse**
- **Risikobewertung** (nichts, Optionen erwägen, Analysen durchführen, Ziele überdenken), Vorlage
- **Risikobehandlung**
- **Überwachen und Überprüfen**

BSI-Standard 200-3

- **Vorarbeiten** zur Risikoanalyse (Informationsverbund, Schutzbedarf, Grundschutzcheck) (200-1, 200-2)
- **Gefährdungsübersicht**: 47 elementare Gefährdungen werden auf die Assets gemappt
- **Risikoeinstufung** über 4x4-Matrix aus Eintrittshäufigkeit / Schadenshöhe
- **Behandlung** von Risiken
- **Konsolidierung** (Überprüfen) (Eignung, Zusammenwirken, Benutzerfreundlichkeit, Angemessenheit, Integration)
- **Rückführung** in den Sicherheitsprozess (BSI 200-2)

Risikoidentifikation

Der Zweck der Risikoidentifikation besteht darin, Risiken **zu finden, zu erkennen und zu beschreiben**, die einer Organisation helfen oder diese daran hindern könnten, ihre Ziele zu erreichen. Relevante, geeignete und **aktuelle** Informationen sind für das Identifizieren von Risiken wichtig.

Faktoren

- Materielle und immaterielle Risikoquellen
- Ursachen und Ereignisse
- ***Bedrohungen und Chancen***
- ***Verwundbarkeiten und Fähigkeiten***
- Änderungen des externen und internen Kontextes
- Indikatoren für aufkommende Risiken
- Art und Wert der Assets und Ressourcen
- Auswirkungen und deren Einfluss auf Ziele
- Einschränkungen in bezug auf Kenntnisse und Verlässlichkeit der Information
- Zeitliche Faktoren
- Voreingenommenheiten, Annahmen und Überzeugungen der Betroffenen

Quellen zur Risikoidentifikation

- Megatrends
- Trends
- Unsicherheiten
- Schwache Signale
- Horizon scanning
- Aufkommende Themen
- "What if" und andere Listen
- …
- Technologie-Roadmaps
- Sinus-Milieus für Zielgruppen, Personas
- Nachrichten, Newsletter
- Ideation (inkl. Brainstorming uvm.)

Beispiel

Risikoidentifikation	Der CEO könnte einen Herzinfarkt haben.
Risikoanalyse	Der CEO teilt keine Informationen (Finanzen, Strategie,…).
	Der CEO ist gesund, aber Risiken könnten bestehen.
Risikobewertung	Der CEO ist ein Single-point of failure (SPOF).
	SPOFs sind für jedes Unternehmen existenziell. **Das Risiko muss behandelt werden.**
Risikobehandlung	a) Der CEO vertraut mehr Mitarbeitern und teilt mehr Informationen.
	b) Der CEO stellt einen Vertreter ein, z.B. einen COO.

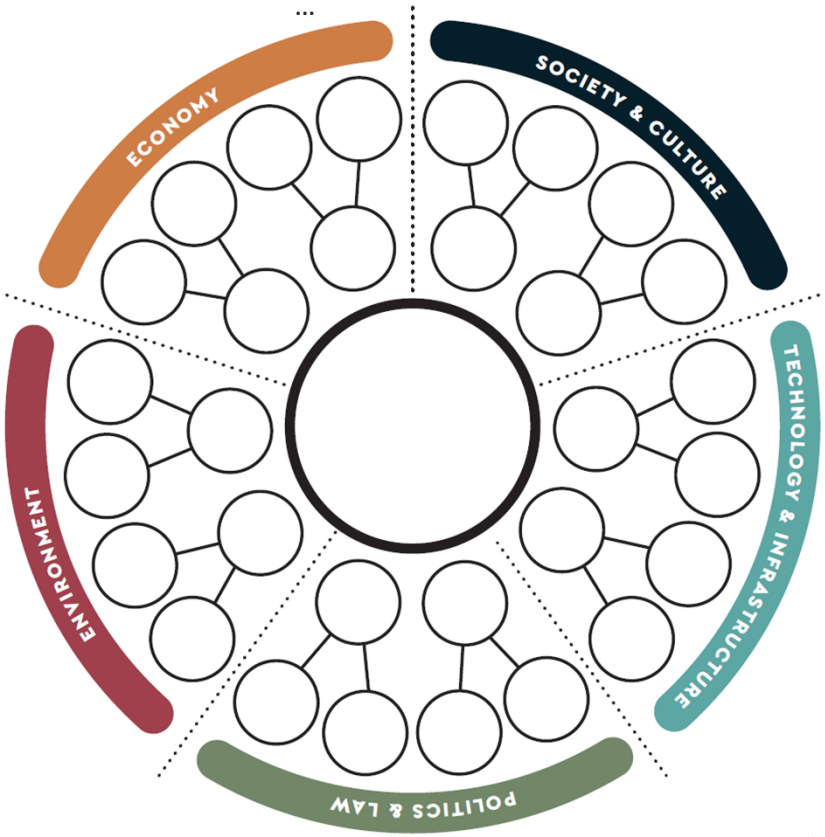
Beispiel für ein Tool zur Risikobeurteilung
Business FutureProofing

MEGATREND

Zunehmende Ressourcenknappheit
Wachsender Einfluss von Ost und Süd
Zunehmende Bedeutung der Migration
+ 11

WHAT IF

Die nächste Zoonose kommt
Ein Shitstorm kommt auf
Der Hauptkunde springt ab
Führungspersonal fällt aus
…



Vorgehensweise

1. **Ausgewählte** Herausforderungen auf ihre **Auswirkungen** überprüfen (FutureWheel, PESTLE-Analyse)
2. **Ausgewählte** Herausforderungen für das **Geschäftsmodell** in einer **Matrix** überprüfen
3. Auf die größten Summen reagieren

	Mega-trend 01	Mega-trend 02	What if 01	What if 02	…	Sum me
Wert-Versprechen	-2	0	2	2		2
Kunden-segmente	2	0	2	2		**6**
Kanäle	1	-2	0	-2		**-3**
Kunden-beziehungen	2	-2	-2	-2		**-4**
…						
Summe	3	**-4**	2	0		

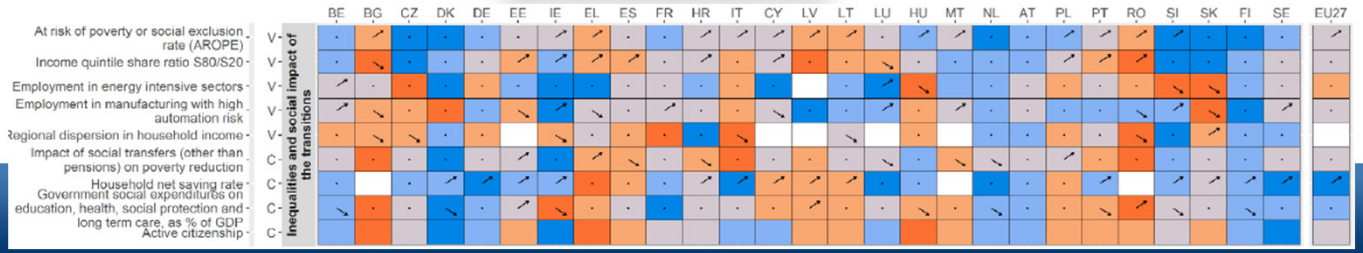
Geschäftsmodell

Quelle der Megatrends: https://knowledge4policy.ec.europa.eu/foresight/tool/megatrends-hub_en oder: https://t1p.de/3lkj9

EU-Kommission und Resilienz

Triple-transition: Digitalisierung, Nachhaltigkeit, Resilienz

- Mit Corona und Ukraine hat das Thema Resilienz in der EU massiv an Bedeutung gewonnen.
- Wichtig u.a.: Strategic Foresight (DG Grow), Horizon scanning, #EUautonomy, NIS2/CER, AI-act
- Bspw.: Supply Chain Alert Notification system, Single Market Emergency Instrument, Recovery and Resilience Facility, Resilienz-Dashboards
- Einsatz des Enterprise Europe Network, um KMU resilienter zu machen



Zusammenfassung

- **Organisationale Resilienz** hängt eng mit dem **IT-Grundschutz** zusammen.
  - Richtig angewandter IT-Grundschutz führt im Kombination mit Risikomanagement für andere Geschäftsbereiche zu organisationaler Resilienz.
  - Unternehmen sollten sich auch auf Business Continuity Maßnahmen vorbereiten.
  - Die Vorgehensweisen des IT-Grundschutzes lassen sich auch auf andere Geschäftsbereiche übertragen.
- Idealerweise geht ein Unternehmen **gestärkt aus einer Krise**. Hierzu sind aber u.a. Vorbereitung, Aufmerksamkeit und Kreativität notwendig. Ein Geschäftsmodell lässt sich z.B. erweitern oder ändern.
- Die **EU-Kommission** legt einen starken Schwerpunkt auf Resilienz. Und nutzt dafür eine Vielzahl von internen und externen Tools, Programmen und Maßnahmen. Auch kleine und mittlere Unternehmen werden unterstützt.

Herzlichen Dank für Ihre Aufmerksamkeit!

Wir freuen uns über Ihre Kontaktaufnahme.

Olaf Jüptner
Innovation, Resilienz, Nachhaltigkeit, Scaleups
HTAI GmbH – EEN Hessen
olaf.jueptner@htai.de
+49-611-95017-8469

Monatlicher Resilienz-Newsletter auf LinkedIn:
https://t1p.de/jiic0

#EENcanhelp