



Kenn ich nicht, mag ich nicht, will ich nicht – Cyber Risk Management, was ist das?

qSkills 2022

Frank Fischer, CISO Deutsche Bahn AG

24.10.2022 | Nürnberg

Cyber Risk Management, was ist das?



← Nicht schmecken, nicht riechen, trotzdem gefährlich?

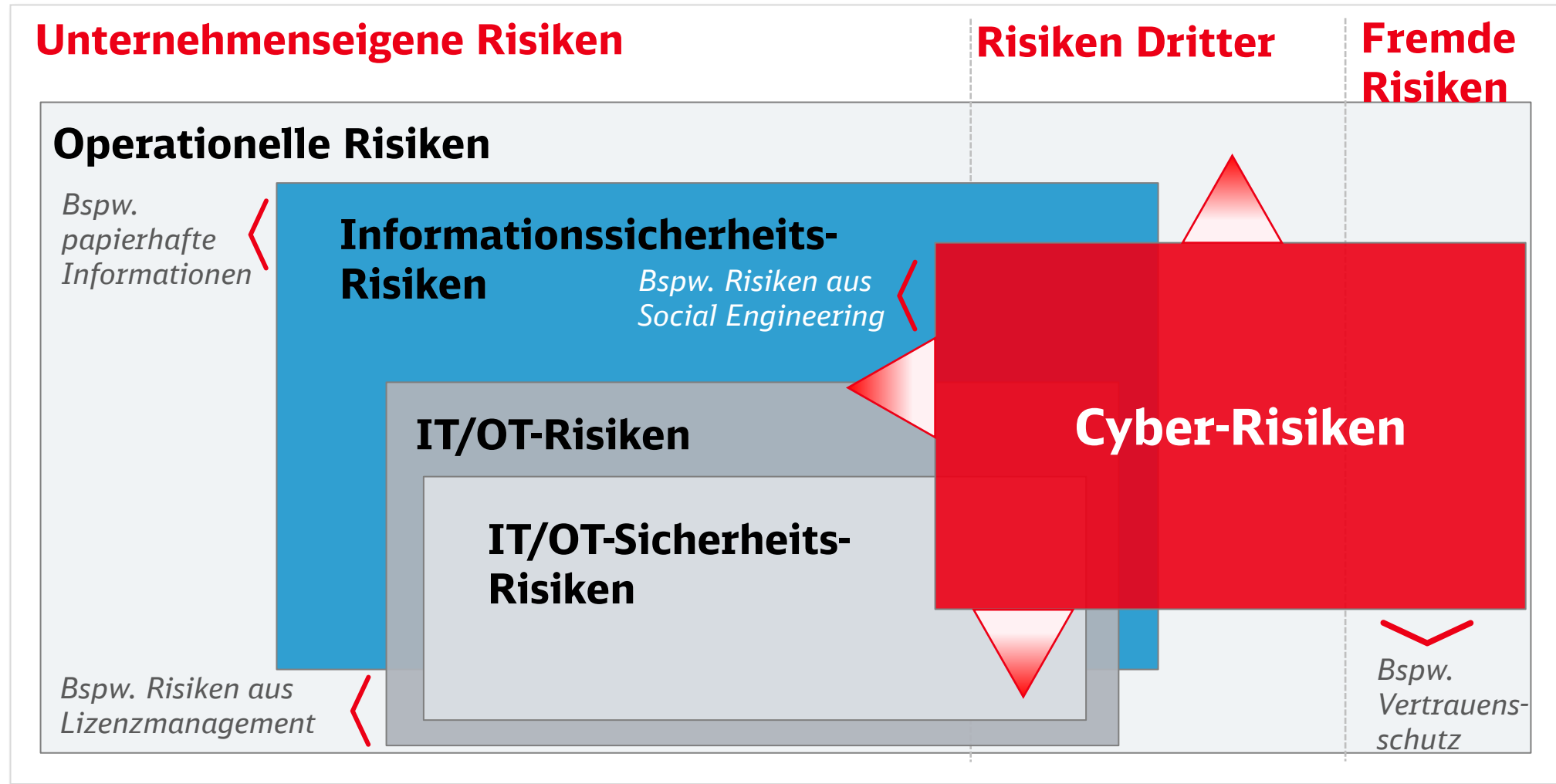
- Einordnung Cyber Risk
- Traditionelles Cyber Risk Management
- Klassische Quantifizierungsansätze
- Herausforderungen bisheriger Vorgehensweisen

→ Mechanismen die für ein nachhaltiges Management essentiell sind

- Iteratives Vorgehen zur Erschließung komplexer Risiken
- Angreifer verstehen heißt Risiken verstehen
- Vollständigkeit auf dem Scheiterhaufen – was tun bei großen Datenlücken?
- Fraktale Quantifizierungs Prozesse verbessern die Genauigkeit

→ → → Schlussfolgerungen

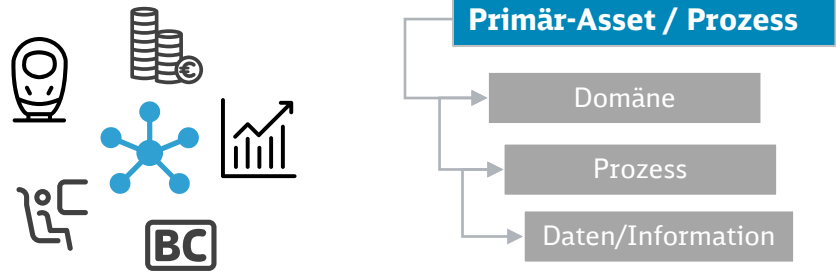
← Nicht schmecken, nicht riechen, trotzdem gefährlich? Risikolandkarte zeigt den Bedeutungsgewinn von Cyber Risiken



← Kenn ich nicht...

Erzeugung des Cyber Risiko Portfolios durch Top-Down Betrachtung

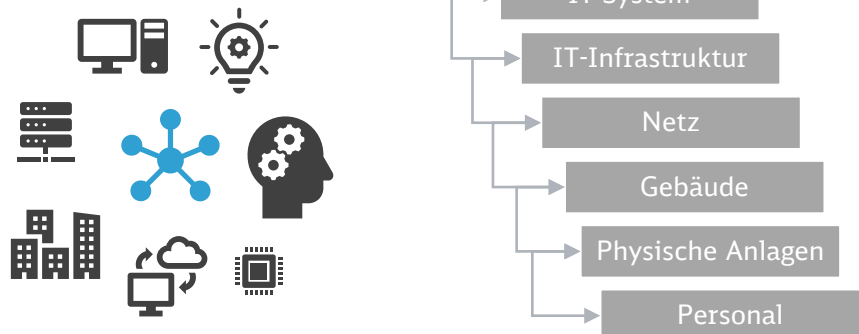
Business / Kunden Orientierung



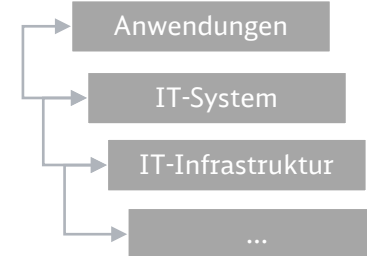
Konzern ISMS / ISMS pro OE



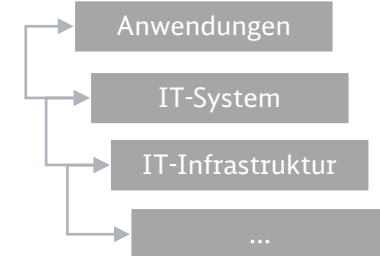
Unterstützende IT/OT Assets



Eigenbetrieb



Service / Dienstleistung



← Mag ich nicht...

Qualitative Risikoermittlung ist die Vorstufe der Quantifizierung

Methodischer Ansatz zur Risikobestimmung nach ISO 27005

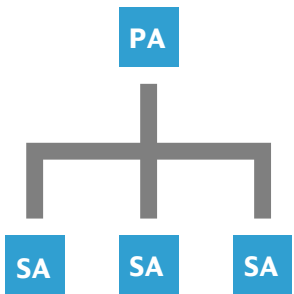
Methodischer Ansatz nach ISO 27005:



Strukturdefinition und Prüfgegenstand



Herstellung des Kontext



Ermittlung des Gesamtschutzbedarf



Prozesse

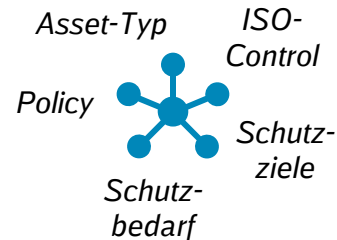


Infrastruktur

Daten aus dem Risk Self Assessment



ISO-Control Katalog



Durchführung der Risikoabschätzung



Szenario-orientiertes Vorgehen auf Primär- und Sekundär-Asset Ebene

Für Schutzbedarf

- Normal
- Hoch
- Sehr Hoch



Durchführung der Risikobehandlung



- Bestimmung von Maßnahmen für die Mitigation von Risiken
- Umsetzungsplanung und Monitoring
- Pflegen des Risikoregisters



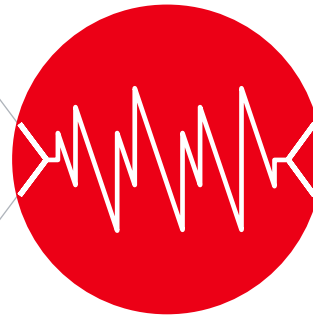
← Will ich nicht...

Klassische Quantifizierung der Risikoszenarien

Ursache (Cause)

- **Operative Beeinträchtigung** des Technologiestacks eines Kernprozesses
- Darstellung potentieller Risiken durch **Schadensausmaß und Eintrittswahrscheinlichkeit** des Schadensereignisses (**Risikoszenario**) bestimmt.

- ⓧ Verfügbarkeit
- ⓧ Integrität
- ⓧ Vertraulichkeit
- ⓧ Safety



IS RISIKO

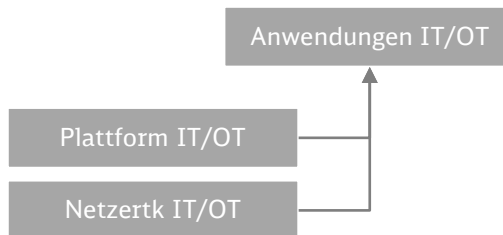
Wirkung (Effect) auf Primär-Asset

- **Ausmaß einer Auswirkung (Schaden)** auf die Geschäftstätigkeiten des Unternehmens.
 - Produkte / Angebotsportfolio
 - Dienstleistungen / Verträge
 - Informationen / Daten
 - Wertschöpfung / Prozesse
- **Verletzung oder Verlust der Vertraulichkeit, Verfügbarkeit und Integrität** von notwendigen Informationen innerhalb des Kernprozesses

Business Stack - Leistungsprozess

Gefährdungsszenario Sekundär-Asset (IT/OT)

- Bedrohung
- Schwachstelle
- Asset-Typ
- Eintrittswahrscheinlichkeit
- mitigierende Maßnahmen



IS-Risikoszenario Primär-Asset

Verfügbarkeit, Integrität, Vertraulichkeit



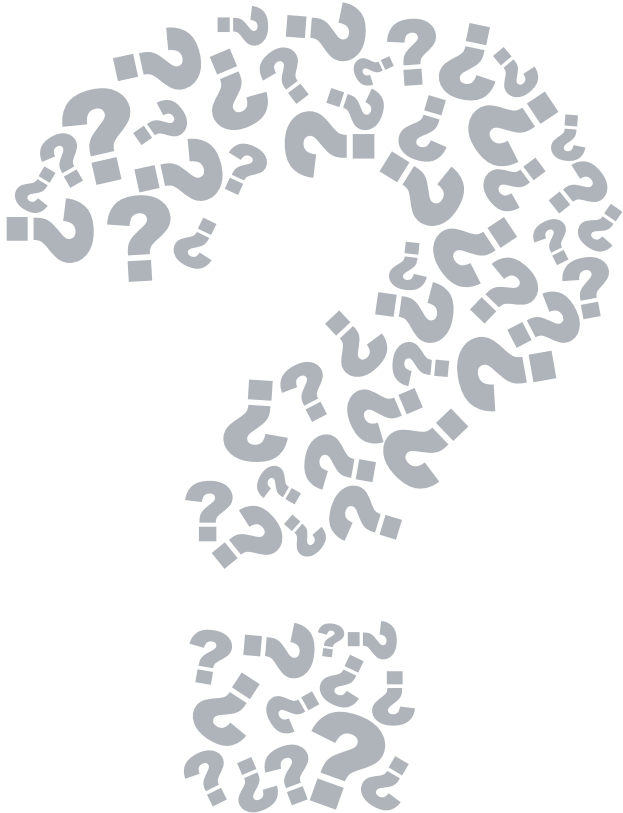
- Bewertung der operative Beeinträchtigung
- Bewertung des reputativen Schadens
- Bewertung des regulatorischen Schadens
- Bewertung von Leib & Leben (betrieblichen Sicherheit (Safety))
- Bewertung des finanziellen Schadens

Prozess

Fähigkeit

Information

← Herausforderungen klassischer Vorgehensweisen, die zur Risikoerhöhung beitragen

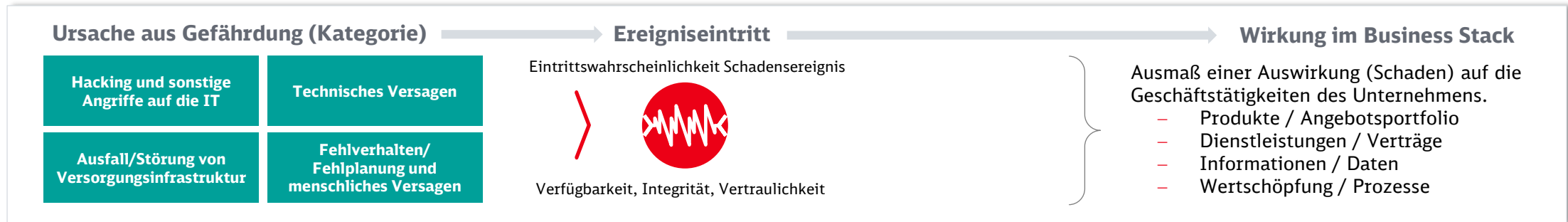


- **Fehlende Referenzierbarkeit der Risiken**
 - Keine referenzierbaren Schadensereignisse
 - Dynamik in der (Asset)veränderung beeinflusst Referenzen
- **Zu wenig Informationen aus der Organisation über**
 - Verletzlichkeit der Prozesse („Hackability“)
 - Widerstandsfähigkeit von Organisation, Prozess und Technik
- **Unbekannte Modifikationen an Vorgaben und Standards**
 - Nicht alle Standards finden effektive Umsetzung
→ Regelungsdefizit
 - Intransparente Regelungsabweichungen → Effektivitätsdefizit
- **Risiko Rohdaten / Szenarios fußen auf falschen Annahmen**
 - Zu allgemeine Verteilungsfunktionen (z.B. Normalverteilung)
 - Falsche/unvollständige Annahmen in der Risikomodellierung

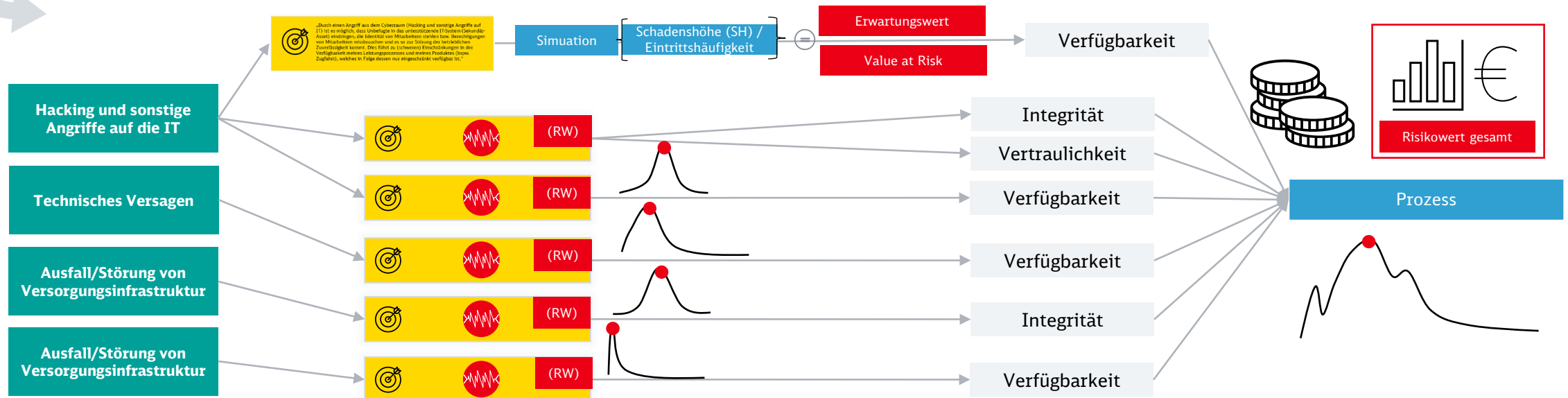
→ Was jetzt?

Iterative Quantifizierung hilft bei der Einschätzung komplexer Risiken

IS-Risikoszenario eines Primär-Assets



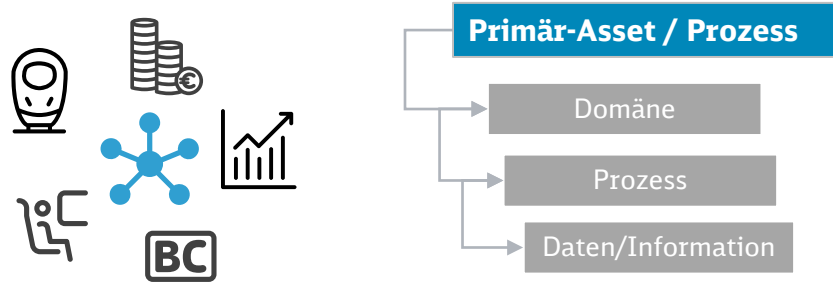
➡ Modellierung von IS-Risikoszenarien für ein Primär-Asset in vier Gefährdungskategorien



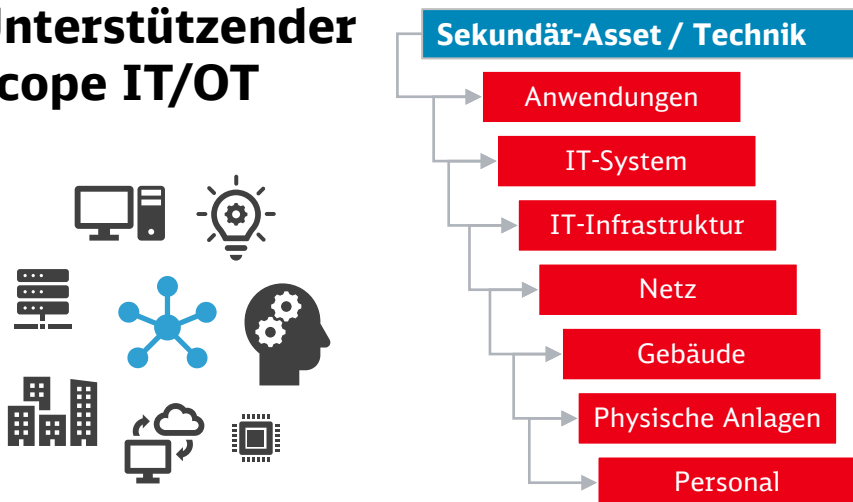
→ Mechanismen die für ein nachhaltiges Management essentiell sind

Komplexitätsreduktion in der Infrastruktur

Business / Kunden Orientierung



Unterstützender Scope IT/OT



– Aufwandstreiber der Risikoermittlung

- **Terminplanung** mit Fachverantwortlichen (medium-hoch)
- Komplexe **Risiko-Modellierung** (siehe Kompensation von Datenlücken) (hoch)
- **Komplexität der Infrastruktur** innerhalb von Kernprozessen (aka „Geltungsbereich“) (hoch-sehr hoch)

– Aufwände in der Infrastrukturanalyse

- **Qualität** vorhandener **BIAs / RIAs**
- Auswertung der **Bedrohungslage**
- **Einschätzung** der eigenen **Widerstandsfähigkeit**
- **Kritische Infrastruktur** Controls

→ **Lösungsansatz : MITRE zur Reduktion der Aufwände in der Infrastruktur**

→ Mechanismen die für ein nachhaltiges Management essentiell sind Komplexitätsreduktion „im Untergrund“



– Angreifer verstehen heißt Risiken verstehen

- **MITRE** liefert eine **wirksame Fokussierung** auf die wahrscheinlichsten Einfallstore
- **Reduktionseffekte** entstehen so auf der **Infrastrukturebene** und aggregieren sich auf der Ebene der Kernprozesse

– Konzentration auf MITRE Schwerpunkte hat Vorteile

- **Kleinere Personengruppe** ist für die Einschätzung der Wahrscheinlichkeiten relevant (**Genauigkeit/Geschwindigkeit+**)
- **Direkte Korrelation** von Risikogröße und Mitigations-Maßnahmen möglich (**Wirksamkeit+**)

Infrastruktur Controls 100% → 20% (-80%) *

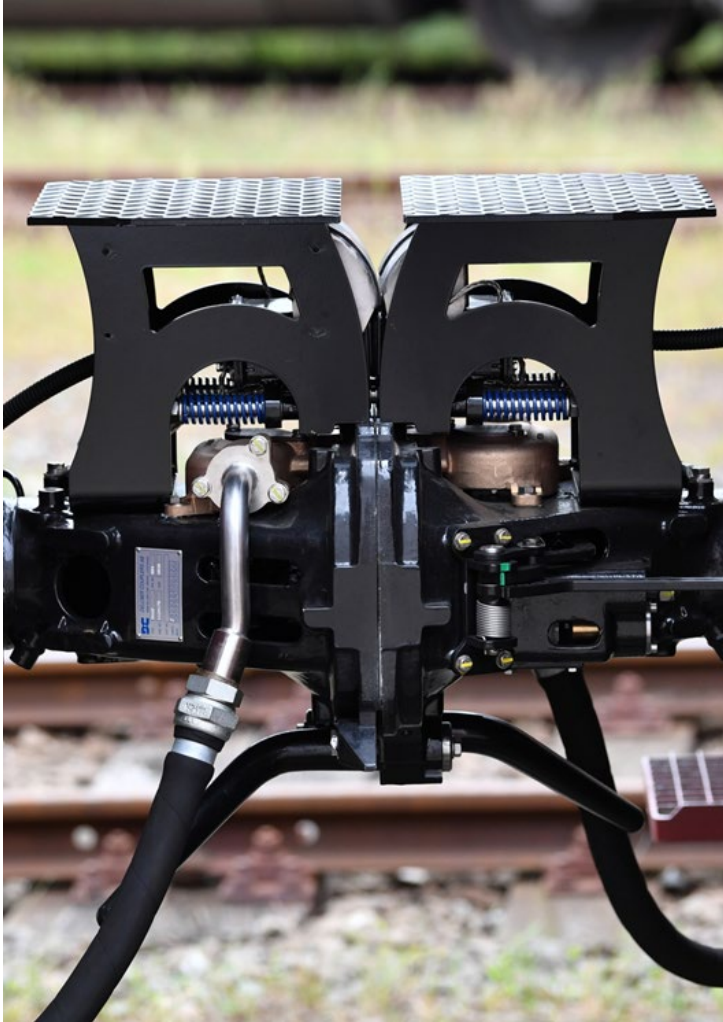
Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 16 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques
Command and Scripting Interpreter (0/8)	Account Manipulation (0/3)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services (0/4)	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)
Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits
Deploy Container	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Credentials from Password Stores (0/5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/2)
Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Debugger Evasion	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Obfuscation (0/3)	Exfiltration Over C2 Channel (0/1)
Inter-Process Communication (0/3)	Browser Extensions	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (1/6)	Browser Session Hijacking	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)
Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deploy Container	Forge Web Credentials (0/2)	Cloud Storage Object Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)
Scheduled Task/Job (1/5)	Create Account (0/3)	Escape to Host	Direct Volume Access	Input Capture (0/4)	Container and Resource Discovery	Software Deployment Tools	Data from Configuration Repository (0/2)	Fallback Channels	Exfiltration Over Web Service (0/2)
Shared Modules	Create or Modify System Process (0/4)	Event Triggered Execution (0/15)	Domain Policy Modification (0/2)	Modify Authentication Process (0/5)	Debugger Evasion	Taint Shared Content	Data from Information Repositories (0/3)	Ingress Tool Transfer	Scheduled Transfer
Software Deployment Tools	Event Triggered Execution (0/15)	Exploitation for Privilege Escalation	Execution Guardrails (0/1)	Multi-Factor Authentication Interception	Domain Trust Discovery	Use Alternative Authentication Material (0/4)	Data from Local System	Non-Standard Port	Transfer Data to Cloud Account
System Services (1/2)	External Remote Services	Hijack Execution Flow (0/12)	File and Directory Permissions Modification (0/2)	Multi-Factor Authentication Request Generation	File and Directory Discovery	Group Policy Discovery	Data from Network Shared Drive	Protocol Tunneling	
User Execution (0/3)	Process Injection	Hide Artifacts (0/10)	Hide Artifacts (0/10)	Network Sniffing	Network Service Discovery	Network Share Discovery	Data from Removable Media	Proxy (0/4)	
Windows Management Instrumentation	Implant External Image	Scheduled Task/Job (1/5)	Hijack Execution Flow (0/12)	OS Credential Dumping (1/8)	Network Sniffing	Network Sniffing	Data Staged (0/2)	Remote Access Software	
	Modify Authentication Process (0/5)	Valid Accounts (1/4)	Indicator Removal on Host (1/6)	Steal or Forge Kerberos Tickets (0/4)	Group Policy Discovery	Group Policy Discovery	Email Collection (0/3)	Traffic Signaling (0/1)	
	Office Application Startup (0/6)	Indirect Command Execution	Indirect Command Execution	Steal Web Session Cookie	Permission Groups Discovery (0/3)	Permission Groups Discovery (0/3)	Input Capture (0/4)	Web Service (0/3)	
	Pre-OS Boot (0/5)	Masquerading (0/2)	Masquerading (0/2)		Process Discovery	Process Discovery	Screen Capture		
	Scheduled Task/Job (1/5)	Modify Authentication Process (0/5)	Modify Authentication Process (0/5)		Query Registry	Query Registry	Video Capture		

Kernprozess Aufwandsminderung mind. -20% (1:4) **

*) Auswertung typischer APT Angriffsstrukturen % Anteil kritischer Controls

**) Schätzung, Schnitt von 4-5 kritische Anwendungen pro Kernprozess

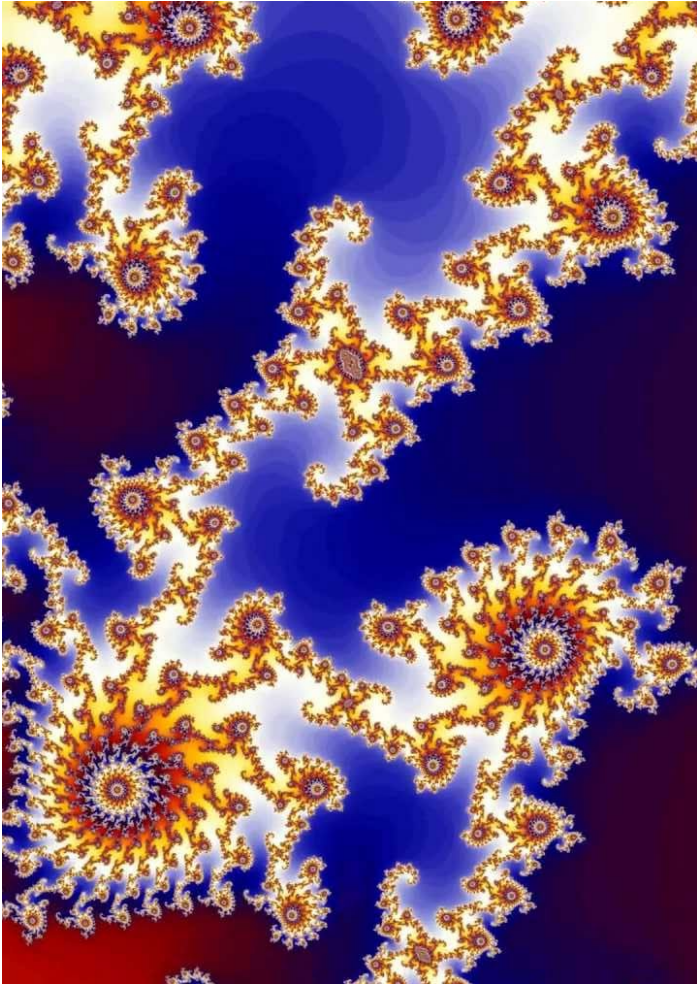
→ Mechanismen die für ein nachhaltiges Management essentiell sind Kompensation von Datenlücken



- **Datenlücke: Vollständigkeit auf dem Scheiterhaufen ??**
 - Fehlende Zusammenhänge in Kernprozessen suggerieren z.T. Unabhängigkeit einzelner Risiken, die aber eigentlich Verbindungen haben
 - Nicht immer sind alle relevanten Assets eines Kernprozesses bekannt
 - Fehlende Schadensereignisse beeinträchtigen Frequenz und Schadensvolumina
- **Lösungsoptionen**
 - Unvollständigkeit reflektiert sich in den Parametern der Simulation
 - Trotz fehlender Daten ist eine erste Risikoabschätzung möglich
- **Aufklärung** von wichtigen Assets mit **Notfall-Ansätzen** (What-If)
- (Monte-Carlo-) **Simulation** mit groben Werten und **geringem Konfidenzintervallen**
- **Inkrementelle Simulationsergänzung** mit nachgeführten Parametern, rekursive Umsetzung des Simulationsverfahrens (siehe Selbst-ähnliche Prozesse)

→ Mechanismen die für ein nachhaltiges Management essentiell sind

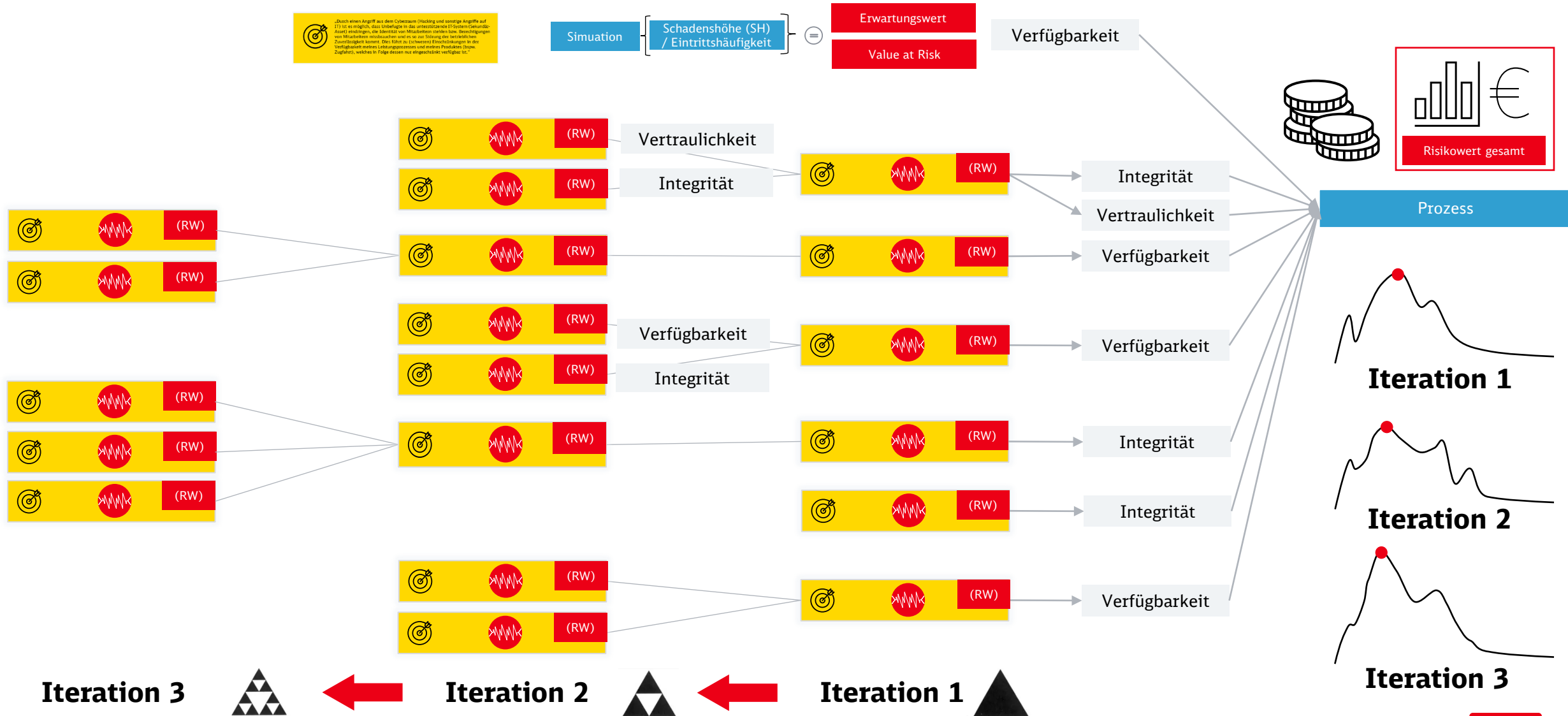
Adaptive (fraktale) Risiko Prozesse



- **Selbstähnliche Risiko-Prozesse verbessern die Genauigkeit**
 - **Fraktale Verteilungsfunktionen** sind nachweislich **genauer** als stetige Verteilungen (Gauß, Bernoulli, Poisson, etc.), die üblicherweise Monte-Carlo-Simulationen zu Grunde liegen
- **Ergänzung der Simulationsalgorithmen**
 - **Selbstähnliche (fraktale) Funktionen** erlauben **schrittweise Verfeinerungen** ohne alle Parameter zu stören (Adaption wo nötig/möglich)
 - Verfeinerung der Simulation **bei Gewinnung weiterer Details** für schrittweise Verbesserung der Schätzung / Konfidenzniveaus
 - Anpassungsfähigkeit **passt besser zur Dynamik** der Risikoentwicklung
- **Schrittweise Annäherung** an den Risikobereich (Range) in der Simulation, ohne alle Daten von Anfang an haben zu müssen, Kompensation von Defiziten klassischer Verteilungen (One-Size-Fits)

Quelle <https://www.youtube.com/watch?v=01kUkiVsuV8>

→ Fraktale (selbst-ähnliche) Verbesserung der Quantifizierung bei Erkenntnisgewinnen



→→→Schlussfolgerungen



- **Cyber Risk Management ist ein wesentlicher Anteil des Operationalen Risikos (OpRisk)**
 - **Cyber Risk gewinnt rasant an Bedeutung** im OpRisk, auch außerhalb der Finanzindustrie
 - **Stochastik ist zwingend erforderlich** um komplexe Wirkzusammenhänge zu schätzen
 - Cyber Risk Quantifizierung ist **essentiell für die Kommunikation** mit Vorstand und Aufsichtsrat
- **Herausforderungen im Cyber Risk Management**
 - **Fehlende Vollständigkeit** der zugrundeliegenden Rohdaten
 - **Fehlende Schadensreferenzen** behindern stabile Risikoszenarien
 - Initiale Schätzung liefern oft **zu hohe Schadenserwartungen** und **zu geringe Häufigkeiten**
- **Maßnahmen die Abhilfe schaffen können**
 - **Stresstests** → Ermittlung der Vollständigkeit der Assetbasis von Kernprozessen
 - **Angreiferdenken** → Komplexitäts –und Aufwandsverringering
 - **Konfidenzmanagement** → fehlende Datenbestände, Datenlücken sind kein Hindernis (Bandbreiten)
 - **Fraktale Risikoschätzungen** → höhere Anpassungsfähigkeit/Qualität von Risikoaussagen

