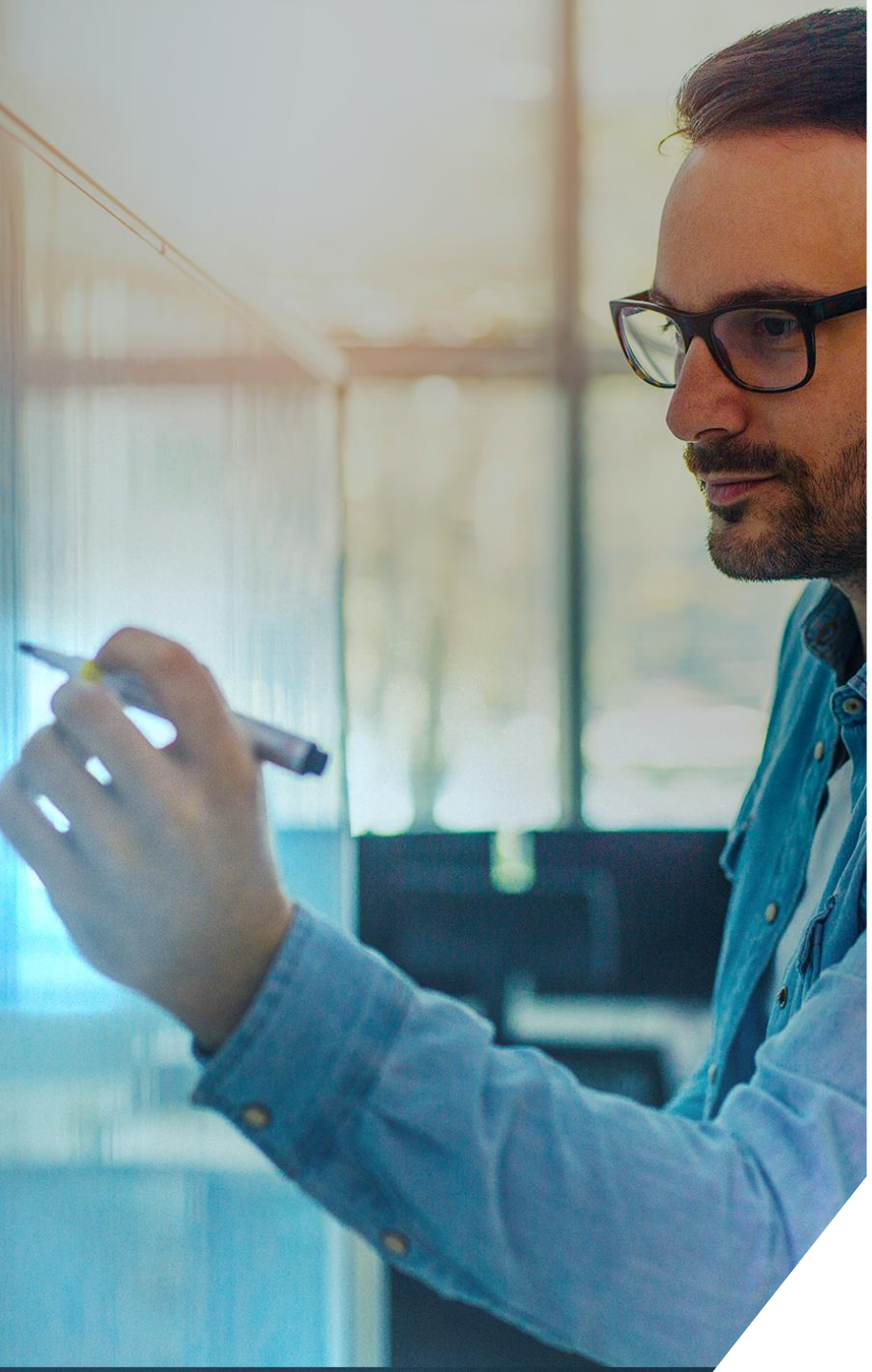
# Resilienz: Der Weg ist das Ziel

Workshop GI-FG SECMGT, 20.03.2026



01 Zur praktischen Bedeutung von Resilienz im Cyberraum:
**Wer oder was soll denn nun resilient sein?**

02 Geforderte Fähigkeiten benötigen zutreffende Ziele:
**Schutzziele für Resilienz**

03 Kontextabhängige Vielfalt bei Anforderungen:
**Praktische Probleme am Beispiel RZ-Dienst**

04 Kontexttypische Umsetzung der Resilienz:
**Beispiele für Resilienz-Maßnahmen**

Zuerst die ausschlaggebende Vorfrage klären:

# Wer oder was soll denn nun resilient sein? (1)

Unabhängig davon, welche Bedeutung „Resilienz“ tatsächlich hat, hängt dessen Ausprägung maßgeblich vom **Schutzgut und dessen Kontext** ab:

- Die **CER-RL 2022/2557** definiert „Resilienz“ im Kontext kritischer Einrichtungen als deren **Fähigkeit,** einen **Sicherheitsvorfall zu verhindern,** sich davor zu schützen, **darauf zu reagieren**, einen solchen abzuwehren, die Folgen eines solchen Vorfalls zu begrenzen, einen Sicherheitsvorfall aufzufangen, zu bewältigen **und sich von einem solchen Vorfall zu erholen**
- Die zeitgleich veröffentlichte **DORA-VO 2022/2554** wiederum definiert „digitale operationale Resilienz“ als die **Fähigkeit** eines Finanzunternehmens, seine **operative Integrität und Betriebszuverlässigkeit aufzubauen, zu gewährleisten und zu überprüfen**, indem es entweder direkt oder indirekt durch Nutzung der von IKT-Drittdienstleistern bereitgestellten Dienste das gesamte Spektrum an IKT-bezogenen Fähigkeiten sicherstellt, die erforderlich sind, um die Sicherheit der Netzwerk- und Informationssysteme zu gewährleisten, die von einem Finanzunternehmen genutzt werden und die kontinuierliche Erbringung von Finanzdienstleistungen und deren Qualität, einschließlich bei Störungen, unterstützen
- In der **ISO 22300:2025** dagegen wird im Kontext von Business Continuity Management „Resilienz“ recht unspektakulär definiert als **Fähigkeit, sich in einem sich verändernden Umfeld anzupassen und Neues aufzunehmen**

**Ergebnis: Resilienz im Cyberraum ist die Fähigkeit**

- **sich auf** i.d.R. rasch, schwer vorhersehbar und i.d.R. nicht direkt beeinflussbar **verändernde Umstände einzustellen** (**„Widerstandsfähigkeit**“ im Rahmen des sog. All-Gefahren-Ansatzes)
- **sich auf** gezielt herbeigeführte als auch **im konkreten Umfeld eintretende Einflüsse** derart **einzustellen, dass die Zuverlässigkeit und Stabilität des Schutzgutes** in ausreichenden Umfang **aufrecht erhalten werden kann** (**„Robustheit**“ gegenüber dauerhaft wirkenden Störungen wichtiger Betriebstätigkeit)

3 Die Cyberresilienz-VO 2024/2847 definiert dagegen nicht, was unter Cyberresilienz zu verstehen ist

Zuerst die ausschlaggebende Vorfrage klären:

# Wer oder was soll denn nun resilient sein? (2)

Resilienz (Widerstandsfähigkeit & Robustheit) kann sich auf verschiedene **Schutzgüter** beziehen:

- **Einrichtung als Ganzes**, wie z.B. einer kritischen Einrichtung (nach CER-RL)
- **Einzelner Standort**, einzelnes Gebäude bzw. einzelner Raum
- **Einzelne operationale Tätigkeit**, wie z.B. von kritischen und wichtigen Funktionen (nach DORA-VO)
- **Einzelne Netz- und Informationssysteme** („Produkte mit digitalen Elementen“)
- **Einzelne Versorgungseinrichtungen** (Strom, Kühlung, Internetzugang, …)
- **Betriebsnotwendiges Personal**
- **Betriebsnotwendige Infrastruktur**
- **Betriebsnotwendige Abläufe**
- **Betriebsnotwendige Information**
- **Betriebsnotwendige Lieferkette**
- **Betriebsnotwendige Fähigkeiten**

**Ergebnis: Für jedes Schutzgut bedeutet Resilienz etwas anderes** und beinhaltet jeweils

- Fähigkeit zur geeigneten & angemessenen Reaktion bei Eintritt eines Fehlerfalls bzw. einer Störung („**Fehlertoleranz**“)
- Fähigkeit zur Begrenzung vorhandener (technischer als auch organisatorischer) Schwachstellen („**Schwachstellenmanagement**“)
- Fähigkeit zur Kontrollierbarkeit & Nachvollziehbarkeit von Schnittstellen („**Datenflusskontrolle**“)
- Fähigkeit, bei Bedarf auf nachgewiesen sichere bzw. gut beherrschte Zustände zurückgreifen zu können („**Fail-Safe-Mechanismus**“)
- Fähigkeit zur Schadensbegrenzung („**Defense in Depth**“)
- Fähigkeit, begründet auf vertrauenswürdigen Einsatz von Netz- und Informationssystemen, Personal bzw. Dritte setzen zu können („**Trusted Services**“)

Resilienz im Cyberraum nur mit umfassenden Zielen zu erreichen:

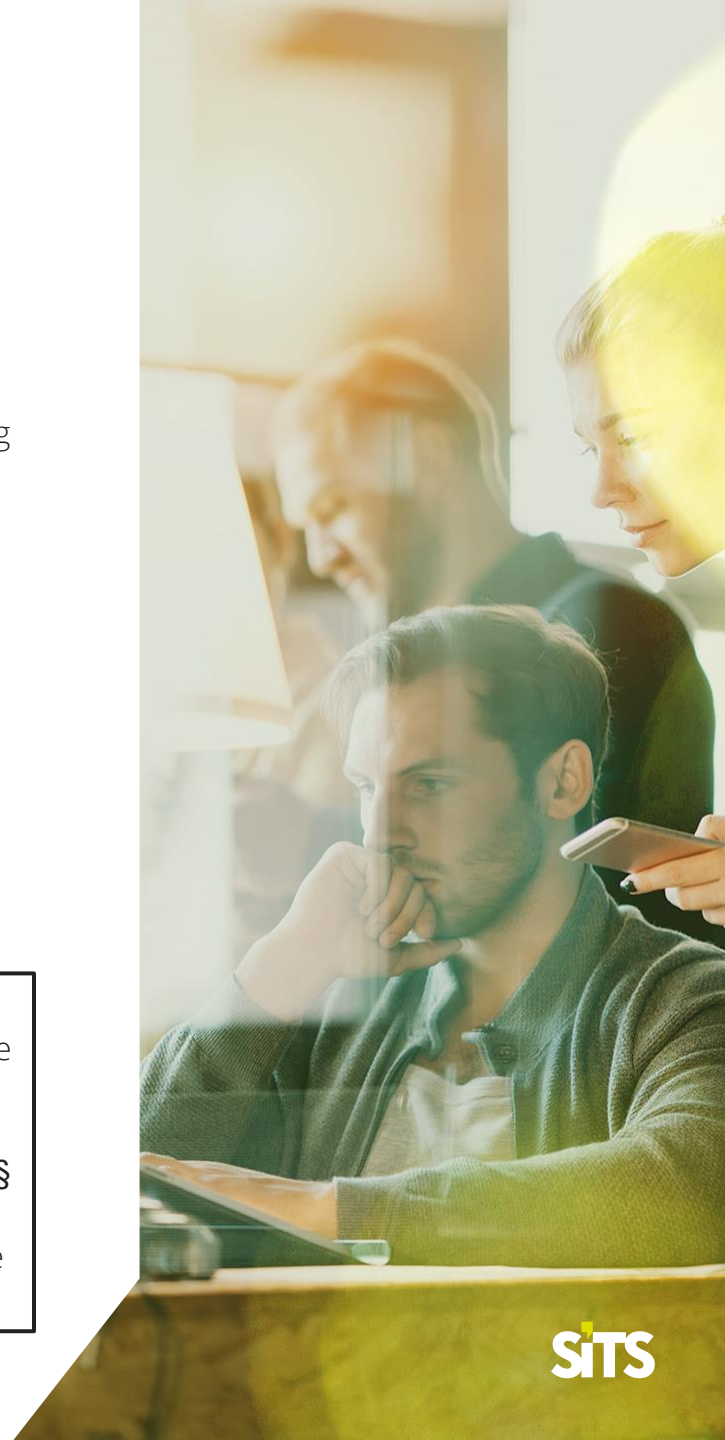
# Schutzziele für Resilienz

Um die zu benötigten Fähigkeiten hinsichtlich des jeweiligen Schutzgutes unter Berücksichtigung der bestehenden Risikoexposition tatsächlich erreichen zu können wird mehr benötigt als Hochverfügbarkeit und Incident Response:

- Nach ErwG 79 der NIS2-RL 2022/2555 sind Maßnahmen zum **Schutz der Netz- und Informationssysteme vor Systemfehlern, menschlichen Fehlern, böswilligen Handlungen oder natürlichen Phänomenen** im Einklang mit europäischen und internationalen Normen wie denen der Reihe ISO/IEC 27000 einzubeziehen
- Ermittelte **Ziele** zu **Widerstandsfähigkeit, Robustheit, Fehlertoleranz, Schwachstellenmanagement, Datenflusskontrolle, Fail-Safe-Mechanismus, Defense in Depth & Trusted Service** sind zweckmäßigerweise dabei entsprechend zu adaptieren
- Neben der zweifellos zentralen **Verfügbarkeit** lässt sich Resilienz nur erreichen mit **Integrität** und **Authentizität** als weiteren zentralen Standpfeilern **sowie** angemessener **Vertraulichkeit** zu Details getroffener Maßnahmen
- **Authentizität** stellt die Echtheit von Daten und Identitäten fest. Sie ist daher **für die Vertrauenswürdigkeit von digitalen Services von größter Wichtigkeit**: Während die Integrität insbesondere die Vertrauenswürdigkeit von Datenbestand bzw. Systemzustand garantiert, wird die Vertrauenswürdigkeit des Auslösers eines digitalen Ereignisses nur durch die Authentizität gewährleistet. Doch ausgerechnet dieses Ziel wurde bei der deutschen NIS2-Umsetzung regelrecht „versteckt“… (*)

**Ergebnis: Lücken aus der Gesetzgebung <u>nicht</u> leichtfertig bei eigener Resilienzplanung ignorieren:**

- Um wirklich resilient sein zu können, sind nicht nur böswillige Handlungen, menschliche Fehler & natürliche Phänomene zu adressieren, wie in der deutschen Umsetzung der CER-RL in § **13 Abs. 3 KRITISDachG** vorgesehen (seit 17.03.2026 in Kraft), sondern auch Systemfehler
- Bei der Maßnahmenplanung keinesfalls ausgerechnet die Authentizität vernachlässigen – entgegen dem Anschein aus § **2 Nr. 1, 17, 39 & 40 BSIG** im Zuge der deutschen Umsetzung der NIS2-RL
- § **30 Abs. 2 BSIG** beschreibt (soweit jedoch konsistent zur NIS2-RL selbst) nur unvollständig benötigte Maßnahmen, die für echte Resilienz benötigt werden





(*) Laut Gesetzesbegründung (S. 130 in BT-Drucksache 21/1501) angeblich ein „Unterfall der Integrität“ (sic!)

# Praktische Probleme am Beispiel RZ-Dienst

## Für RZ-Dienst (bei Überschreitung der Schwellwerte) NIS2-DVO 2024/2690 verbindlich

Nach ErwG 20 gehören zu den **grundlegenden Verfahren**:

- Zero-Trust-Grundsätze
- Software-Updates
- Gerätekonfiguration
- Netzwerksegmentierung
- Identität- & Zugriffsmanagement
- Sensibilisierung der Nutzer
- Clean Desk & Clear Screen
- MFA
- Sicherer Umgang mit E-Mails & Web-Browser
- Sicheres Home Office

Ferner detaillierte Vorgaben im Anhang, die umzusetzen sind

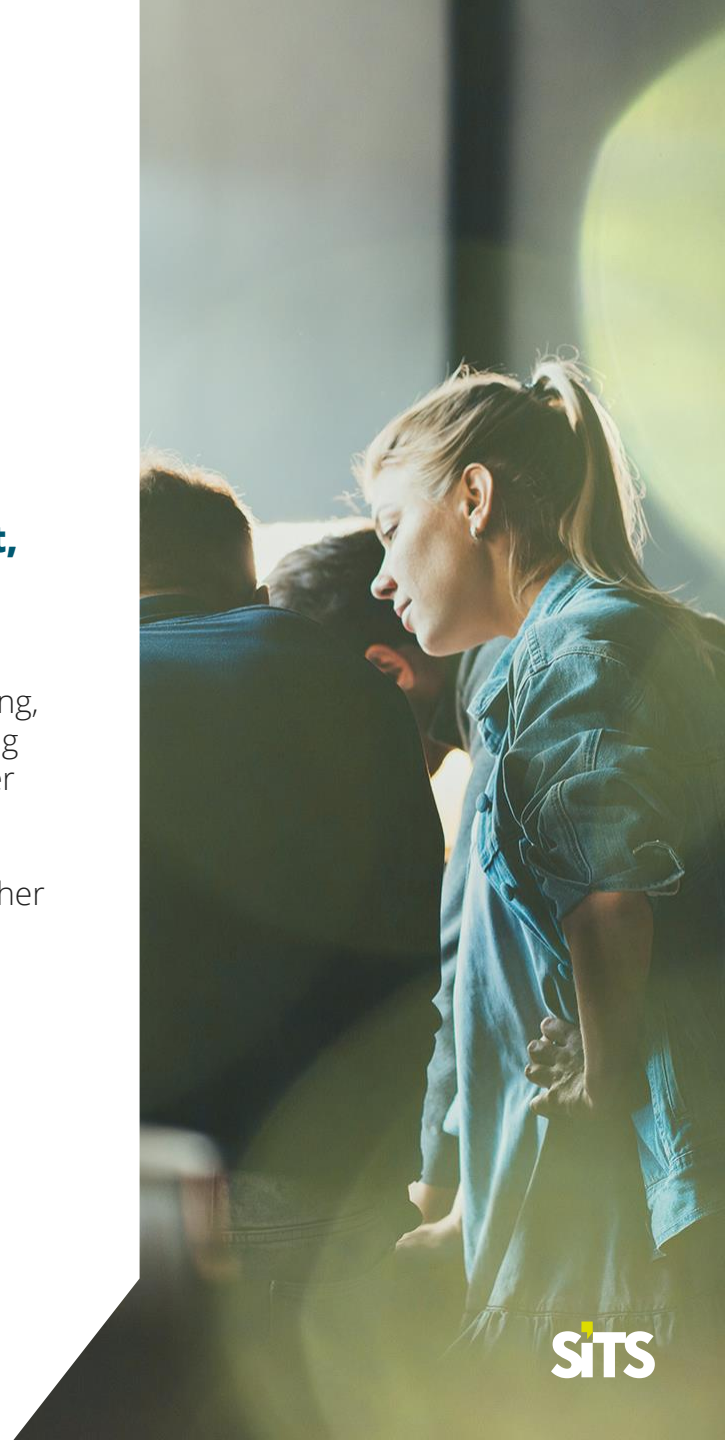
## Bei RZ-Dienst für Finanzunternehmen zudem zahlreiche weitere DORA-VO zu beachten, da durchgereicht

- Benennung der Fristen für zu leistende Unterstützungsdienstleistungen (Art. 4 *)
- Mitteilung über Schwachstellen & Patching (Art. 10 *)
- Aufrechterhaltung der digitalen operationellen Resilienz (Art. 11 *)
- Einhaltung relevanter Vorgaben (Art. 19 *)
- Zuweisung eindeutiger Identitäten (Art. 20 *)
- Test-Durchführung (Art. 25 *)
- Vorfalls-Meldung (Art. 7 **)

## Für RZ-Dienst diverse ISO-Standards relevant, insb. ISO/IEC 27001 ***

Davon mit Bezug zur Resilienz:

- **A.5.30**: Planung, Umsetzung, Aufrechterhalten & Prüfung der IKT-Bereitschaft auf der Grundlage von Business-Continuity-Zielen
- **A.5.14**: Absicherung jeglicher Informationsübertragung
- **A.5.19 – A.5.22**: Beherrschung relevanter Risiken
- **A.8.12**: Verhinderung von Datenlecks
- **A.8.14**:: Redundanz informationsverarbeitender Einrichtungen





* Delegierte VO 2024/1774; ** Durchführungs-VO 2025/302; *** sowie ISO/IEC 22237-7 (Upgrade zur EN 50600-3-1)

Am Beispiel eines RZ-Dienstes:

# Beispiele für Resilienz-Maßnahmen

**Bei Umsetzung des aktuellen Stands der Technik potenziell hilfreich:**

- **Robustheit & Fehlertoleranz**: Hardware / Versorgungstechnikkomponenten aus unterschiedlichen Serien (und wenn möglich von unterschiedlichen Herstellern) beziehen
- **Widerstandsfähigkeit & Datenflusskontrolle & Defense in Depth**: Netzsegmentierung (verschiedene VLANs + DMZs) plus kryptographisch sowie mittels MFA abgesicherter Zugang der Kunden bzw. von Admins über verschiedene, gehärtete & kontrollierte Sprung-Server
- **Robustheit & Schwachstellenmanagement & Fail-Safe-Mechanismus**: Erstellung eines mittels automatisiertem Test nachgewiesenermaßen fehlerfreien & stabil funktionierenden Golden Images, welches als Basis für neue Serversysteme eingespielt werden kann
- **Widerstandsfähigkeit & Schwachstellenmanagement & Defense in Depth**: Regelmäßiger Scan auf Schwachstellen mit besonderem Fokus auf potenziell unübliches Verhalten und relevanten Angriffspfaden unter Berücksichtigung ihrer Ausnutzbarkeit (EPSS neben CVSS)
- **Widerstandsfähigkeit & Defense in Depth & Trusted Service**: Einsatz zweier SOC mit unterschiedlichem Fokus & verschiedenen Datenquellen, die ausgewertet werden, sowie eines Security Engineers, der Ergebnisse beider SOC analysiert und auf zusätzlich feststellbare Auffälligkeiten prüft

**Ergebnis:**

- **Zahlreiche Ziele lassen sich mit einer einzelnen Maßnahme adressieren**
- **Für einzelne Ziele für wirksame Abdeckung jedoch mehrere Maßnahmen nötig**
- **Verwendung von Design-Pattern zu Cybersecurity by Design hilfreich**
- **Leider ist der Weg mühsam & Ressourcen beschränkt – Resilienz keine Kurzstrecke…**

# Bernhard C. Witt

Prinicipal on Cybersecurity and
Critical Entities Protection

Mail: bernhard.witt@sits.com


**Erfahrung & Ausbildung:**

- 25+ Jahre IT & Security Erfahrung
- Diplom-Informatiker und Industriekaufmann
- Seit 2011 in Normung von IT-Sicherheitsverfahren tätig
- Erfahrener ISO/IEC 27001 Lead Auditor
- Prüfer nach § 39 Abs. 1 BSIG
- Autor von Fachbüchern und Fachbeiträgen zur Cybersicherheit

**Aktuelle Fokus-Themen:**

- NIS2-Richtlinie
- DORA-Verordnung
- Schutz kritischer Infrastrukturen

**Was ich sonst so mache:**

- Brett- und Kartenspiele
- Fußball und Snooker schauen
- Lesen

# Vielen Dank für Ihre Aufmerksamkeit!