MAX PLANCK GESELLSCHAFT

RINGVORLESUNG

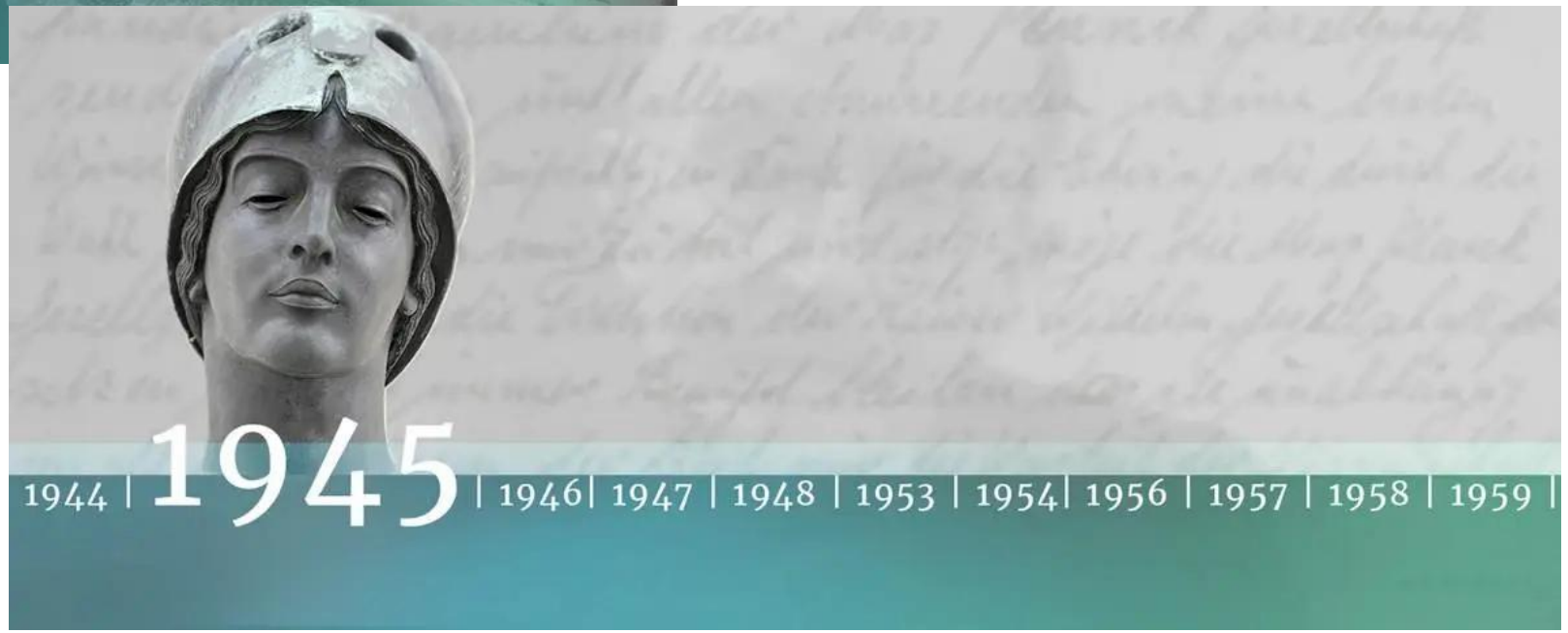
HAW HAMBURG

Guntram Rupp

Informationssicherheitsbeauftragter

20.01.2026

Nach der deutschen Kapitulation im Mai 1945 begannen die Siegermächte, das deutsche Forschungssystem neu zu ordnen.



MAX PLANCK GESELLSCHAFT

Göttingen, 26. Februar 1948
die Wiege der modernen MPG

MAX-PLANCK-GESELLSCHAFT QUICK FACTS

84
MPG Institute & Einrichtungen

4
MPI im Ausland

19
Max Planck Center
u.a. in USA, UK, Japan

28
Nobelpreise
31 Nobelpreisträger*innen

5. Platz
Nature Publishing Index

Top 25
Top Global Innovators von Thomson Reuters

26.000
Beschäftigte
(Personal Gesamt)

2,2 Mrd. €
Budget
(Zuschüsse Bund/Länder 2024)

8.100
Nachwuchswissen-schaftler*innen aus aller Welt

200
Start-ups (seit 1990)

134
Erfindungen (2024)

1. Platz
Beliebtester Arbeitgeber in den Naturwissenschaften

STANDORTE DER 84 MAX-PLANCK-INSTITUTE & EINRICHTUNGEN

Stand: 01/2025

- Institut / Forschungsstelle
- Teilinstitut / Außenstelle
- Sonstige Forschungseinrichtungen
- Assoziierte Forschungseinrichtungen

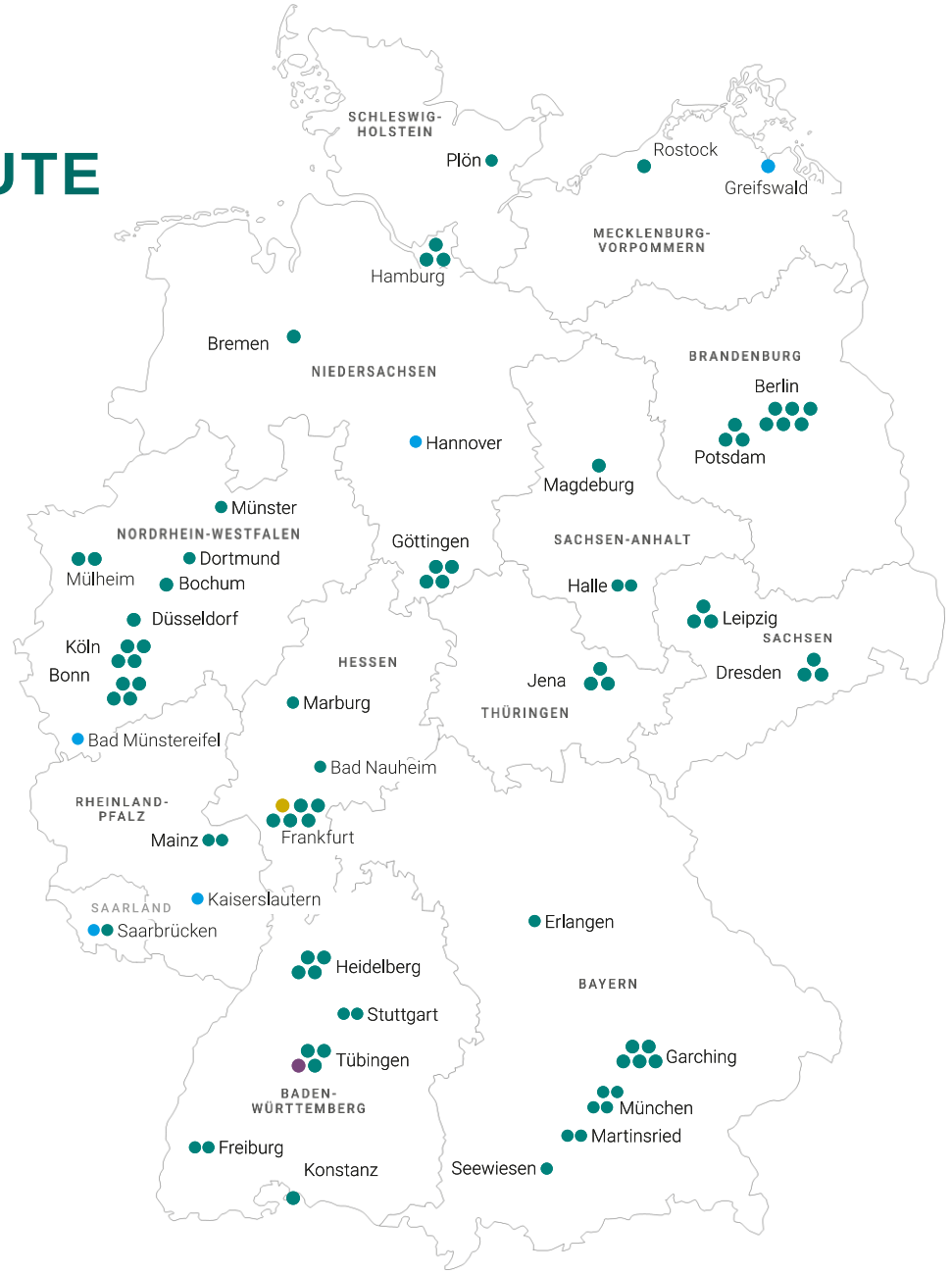
MAX-PLANCK-INSTITUTE IM AUSLAND

Niederlande
- Nimwegen

Italien
- Rom
- Florenz

USA
- Jupiter, Florida

Brasilien
- Manaus



Welche Bederohungen wirken auf eine Wissenschaftseinrichtung?

Wissenschaftsspionage

Bundesamt für Verfassungsschutz

....sorgen für Auszeichnungen....

The People's Republic of China Friendship Award

Awarded for	Foreign experts who have made outstanding contributions to the country's economic and social progress
Location	Beijing
Country	People's Republic of China
Presented by	State Administration of Foreign Experts Affairs State Council of the People's Republic of China

- 2016 Ehrenprofessur, Jiangxi Agricultural University, Nanchang City, China
- 2012 Freundschaftspreis der Volksrepublik China, China
- 2012 Lushan Friendship Award, Jiangxi Provincial Government, China

CYBER-INCIDENTS & NEW TECHNOLOGIES

ZERO-DAY ANGRIFFE TREND 2025

Fokuswechsel der Angreifer: Mehr Angriffe auf Enterprise-Appliances (Firewalls, VPNs, Storage, Hypervisoren) und Cloud-Dienste statt nur Endgeräte.

Bevorzugte Techniken: Remote Code Execution (RCE), Privilege Escalation und Manipulation auf Boot-/Firmware-Ebene für langlebige Persistenz.

Schnelleres Ausnutzen: Durchschnittliche Time-to-Exploit ≈ 5 Tage nach Offenlegung → mittels KI ≈ 5 Stunden nach Offenlegung

Angreifergruppen: Sowohl Staaten (Nation-State-Akteure) als auch Cyberkriminelle (inkl. Ransomware-Banden) nutzen Zero-Days verstärkt gegen Unternehmen und kritische Infrastruktur.

DEEP FAKE

Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

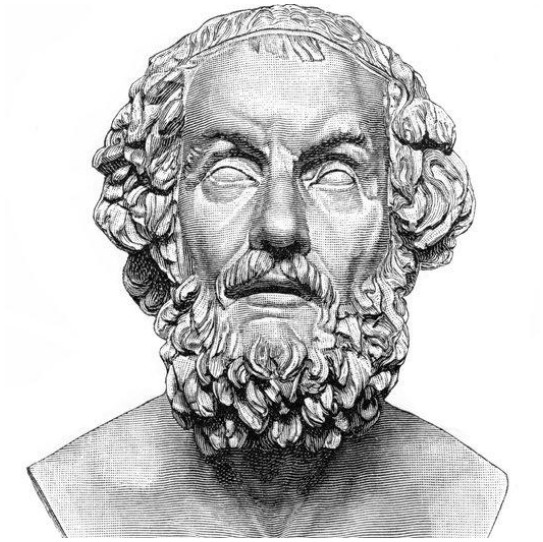
By Heather Chen and Kathleen Magramo, CNN
2 minute read · Published 2:31 AM EST, Sun February 4, 2024

Das Threat Intelligence Team von Okta hat aufgedeckt, wie nordkoreanische Staatsagenten mit Hilfe generativer KI an Jobs in westlichen Unternehmen gelangen – mit dem Ziel, das Regime in Pjöngjang zu unterstützen.
(Bild: Midjourney / KI-generiert)

CYBER - SECURITY

- Herleitung des Begriffs „Cyber“
- Sprachliche Herausforderung

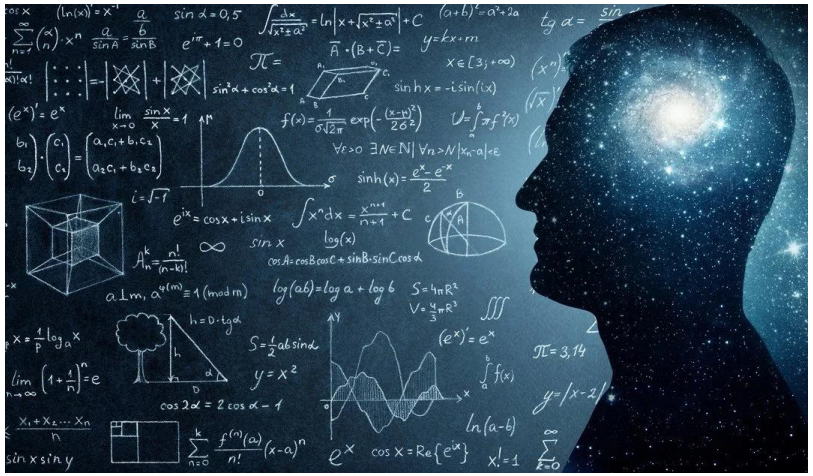
URSPRUNG DES BEGRIFFS “CYBER”



κυβερνήτης
HOMER: Steuermann eines Schiffes

κυβέρνησις
APOSTEL PAULUS im 1. Korintherbrief (1 Kor 12,28 EU),
„Fähigkeit zu leiten“

WISSENSCHAFTLICHE VERWENDUNG VON “CYBER”



Kybernetic / **cybernetics** = “wissenschaftliche Forschungsrichtung“

Wissenschaftliche Etablierung durch den Mathematiker Norbert Wiener im 20. Jahrhundert:
Kybernetik: Wissenschaft und Steuerung in Lebewesen und Maschinen

ERSTE VERWENDUNG VON “CYBER” IM COMPUTER – BEREICH

Control Data CDC1700, Rechenzentrum ETH Zürich, 1975
Archivperlen: Ein 60-Tonnen-Computer für die ETH Zürich – Departement Informatik | ETH Zürich

“CYBER“ Produktlinie von Supercomputern
Gebaut 1971-1989 von Control Data

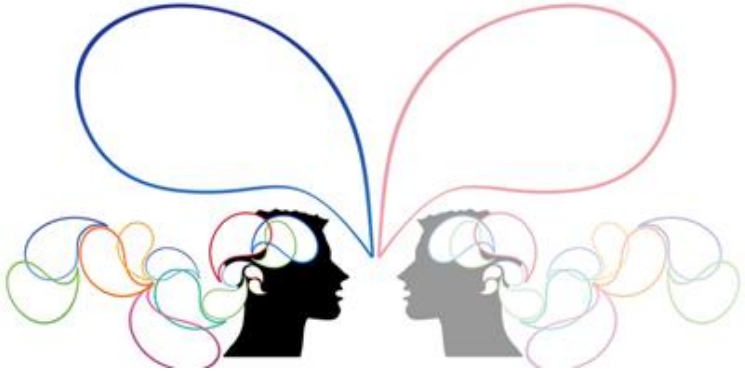
CYBER-SECURITY EINE SPRACHLICHE HERAUSFORDERUNG?

Betonung der verwendeten **Sprachelemente** liegt auf:

- **Technik unter Verwendung von Akronymen**

  AV, SIEM, DLP, DevSecOps, …

WAS LÖST DER BEGRIFF CYBER-SECURITY AUS



„technische Sprache“ wirkt kompliziert!

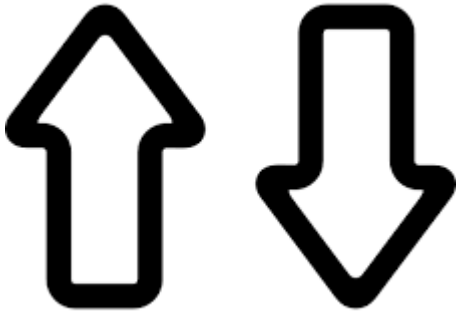
Führungskräfte verstehen diese Sprache oft nicht!

Delegation der Verantwortung für Cyber-Risiken an IT-Teams.

FRAGE: WIE BEKOMME ICH DIE VERANTWORTUNG WIEDER DORTHIN ZURÜCK WO SIE HINGEHÖRT

Rolle rückwärts

VERLAGERUNG VON IT-ANGELEGENHEITEN AUF ORGANISATORISCHES UNTERFANGEN



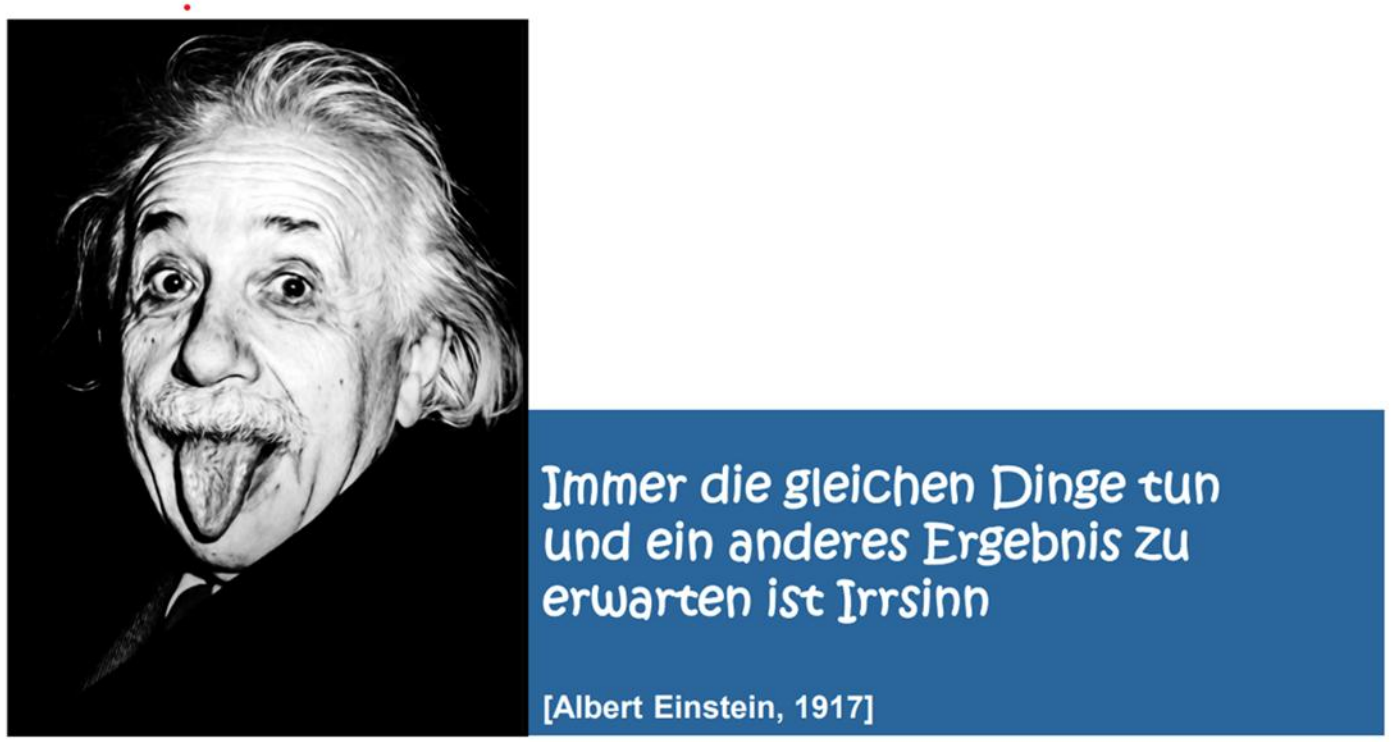
Ziel einer Organisation ist es:

- Vermeidung von Cyber-Angriffen
- Verbesserung der Fähigkeiten:
  - die Auswirkungen eines Angriffs zu minimieren
  - sich schnell von Angriffen erholen zu können
  - sich in diesem Prozess kontinuierlich weiterzuentwickeln

➢ Verwendung des Begriffs Cyber-Resilienz
= die Fähigkeit einer Organisation Cyber-Angriffe:

- zu antizipieren,
- ihnen standzuhalten
- auf sie zu reagieren
- sich ihnen anzupassen

WIE KANN EIN WEG DAHIN SEIN?



CYBER - RISIKO

Cyber

Im Zusammenhang mit Computern, Informationstechnologie oder elektronischer Kommunikation (im Internet befindlich)

Die von Computern erzeugte virtuelle Scheinwelt

Risiko

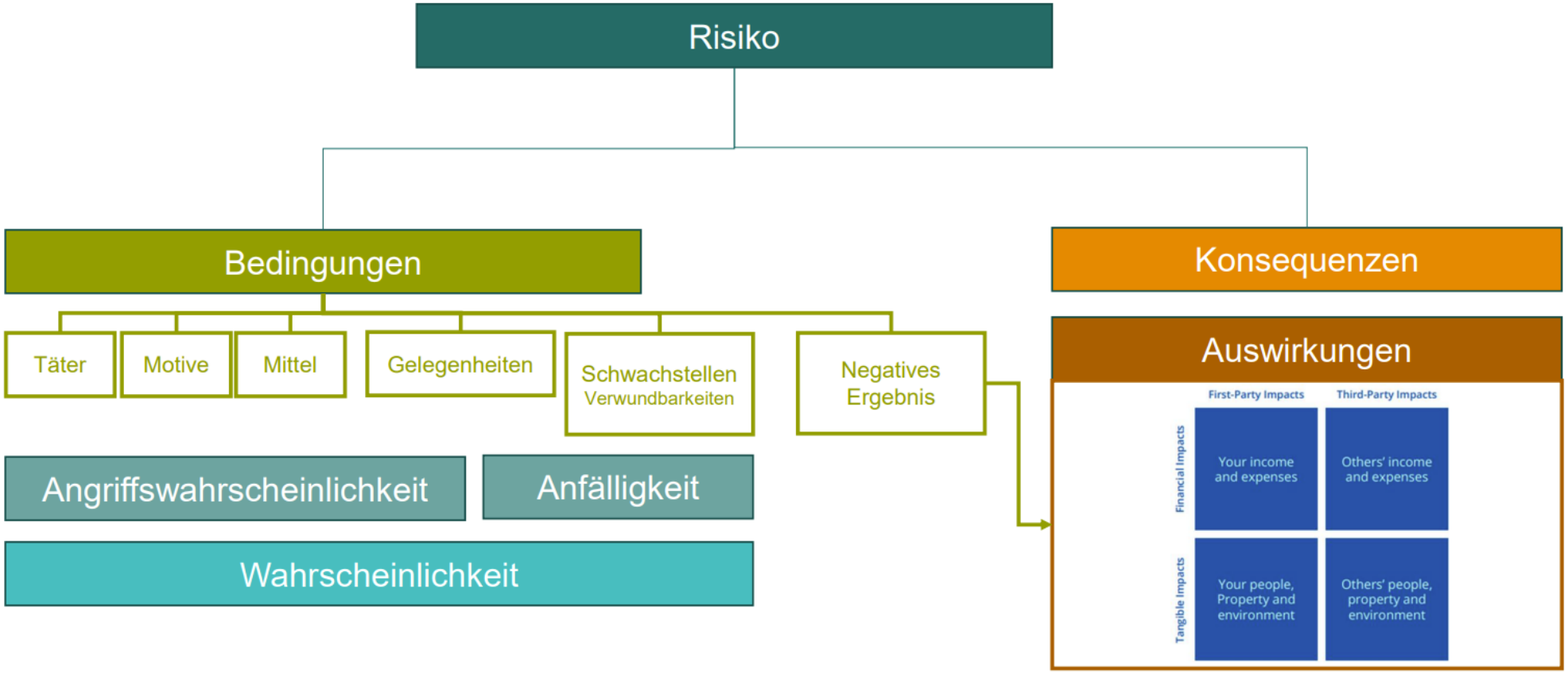
Gefährdung durch Gefahr, Schaden oder Verlust

Cyber Risiko

Gefährdung, Schädigung oder Verlust im Zusammenhang mit der Nutzung von Computern oder durch die Abhängigkeit von Computern, elektronischen Daten oder elektronischer Kommunikation (einschließlich Internet).

Es handelt sich um eine umfassende Betrachtung der potenziellen Gefährdung durch interne Sicherheitsmängel im Zusammenhang mit externen Bedrohungen.

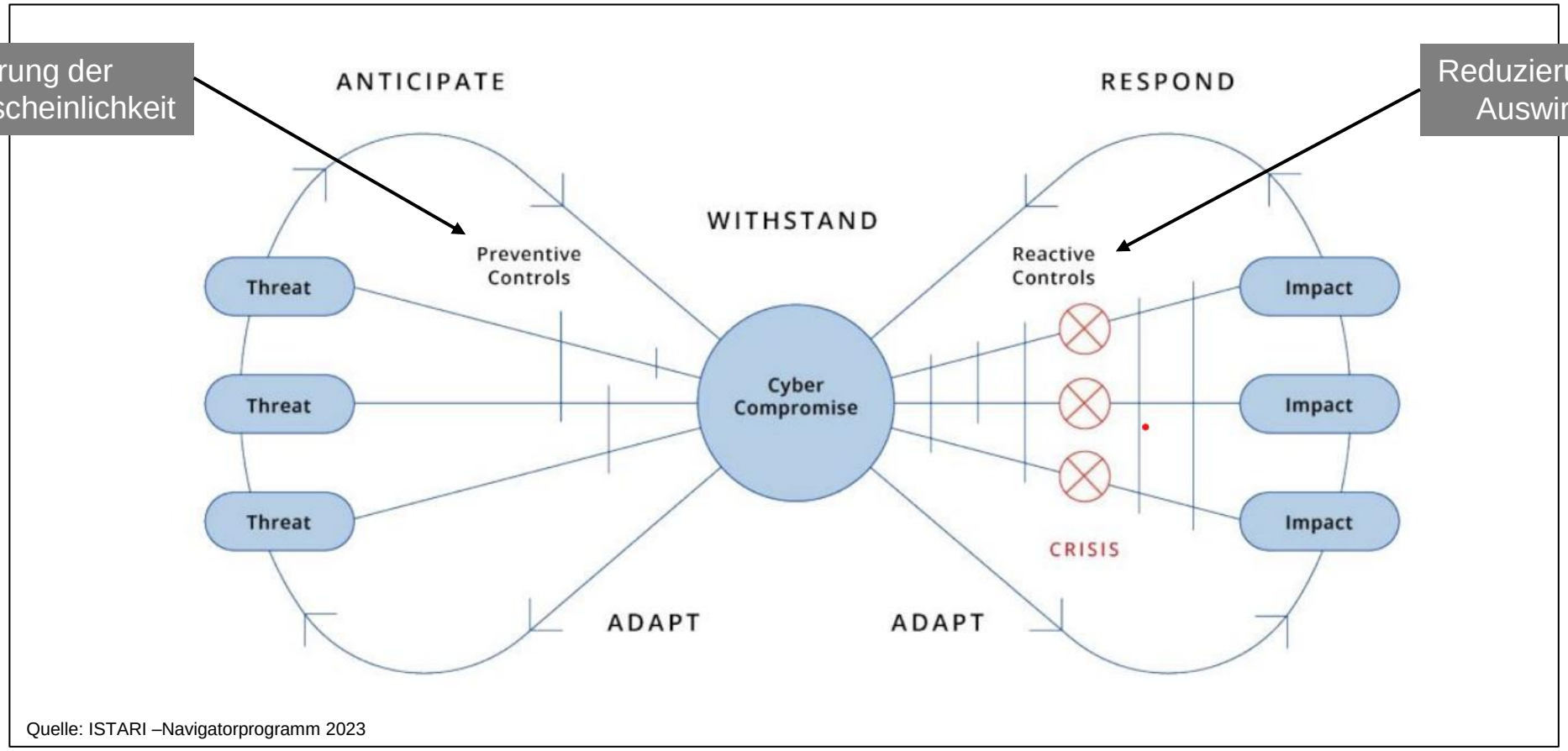
RISIKO - BETRACHTUNGSWEISE



DAS SCHLEIFEN-MODELL (BOW-TIE MODEL)

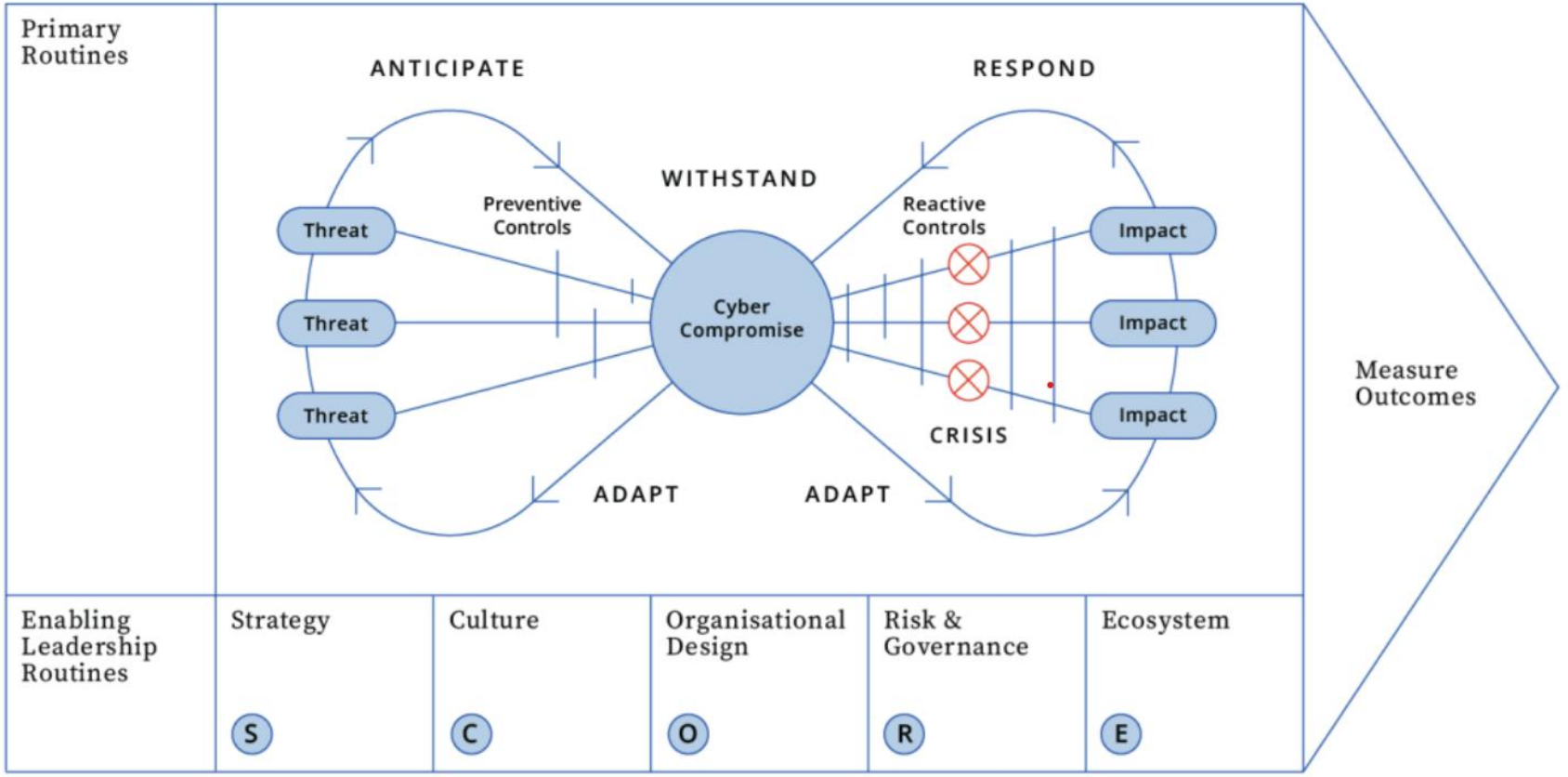
Reduzierung der Eintrittswahscheinlichkeit

Reduzierung der Auswirkung



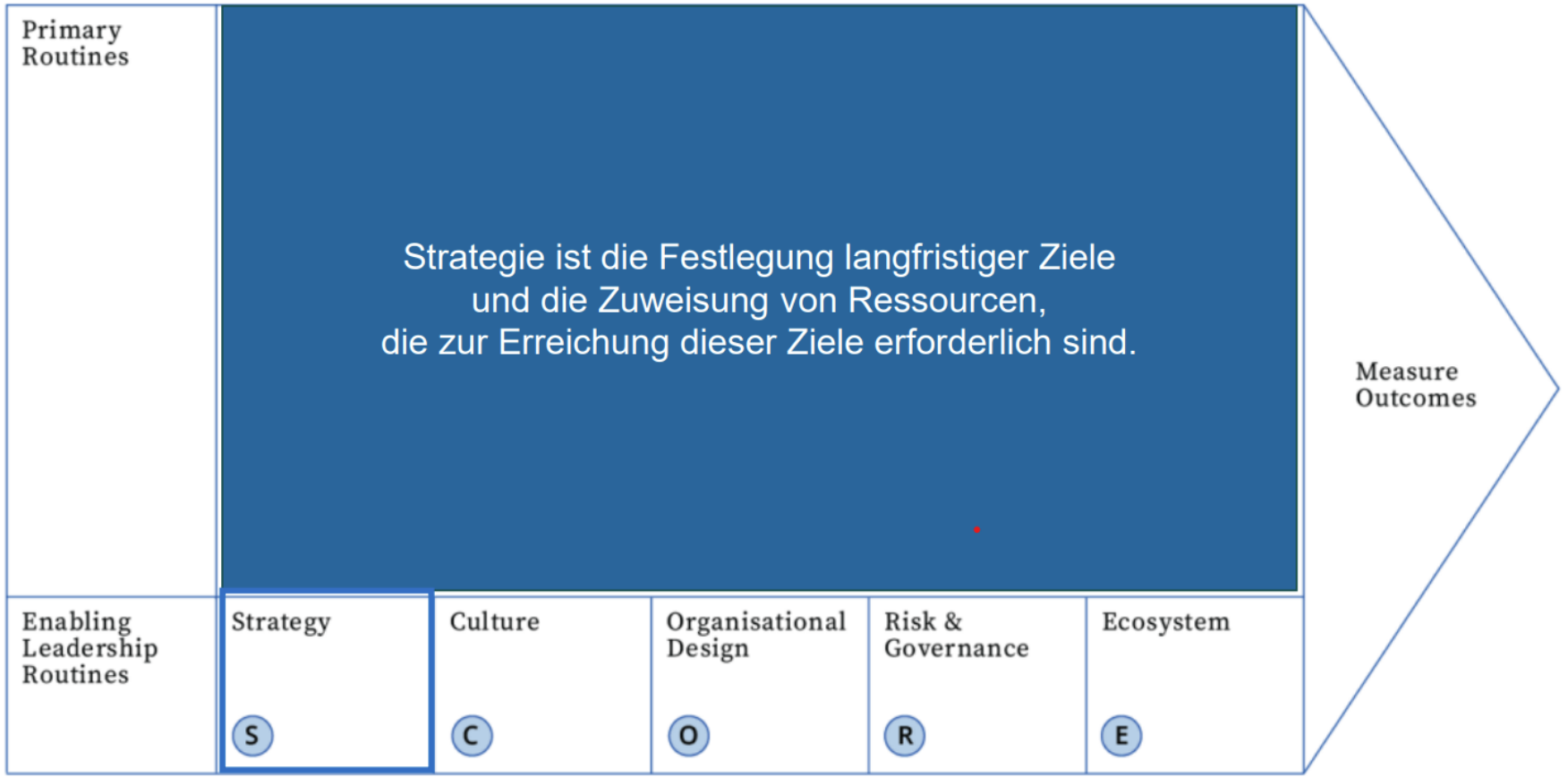
Quelle: ISTARI –Navigatorprogramm 2023

EINBETTUNG DES SCHLEIFEN-MODELL IN EINE ORGANISATION

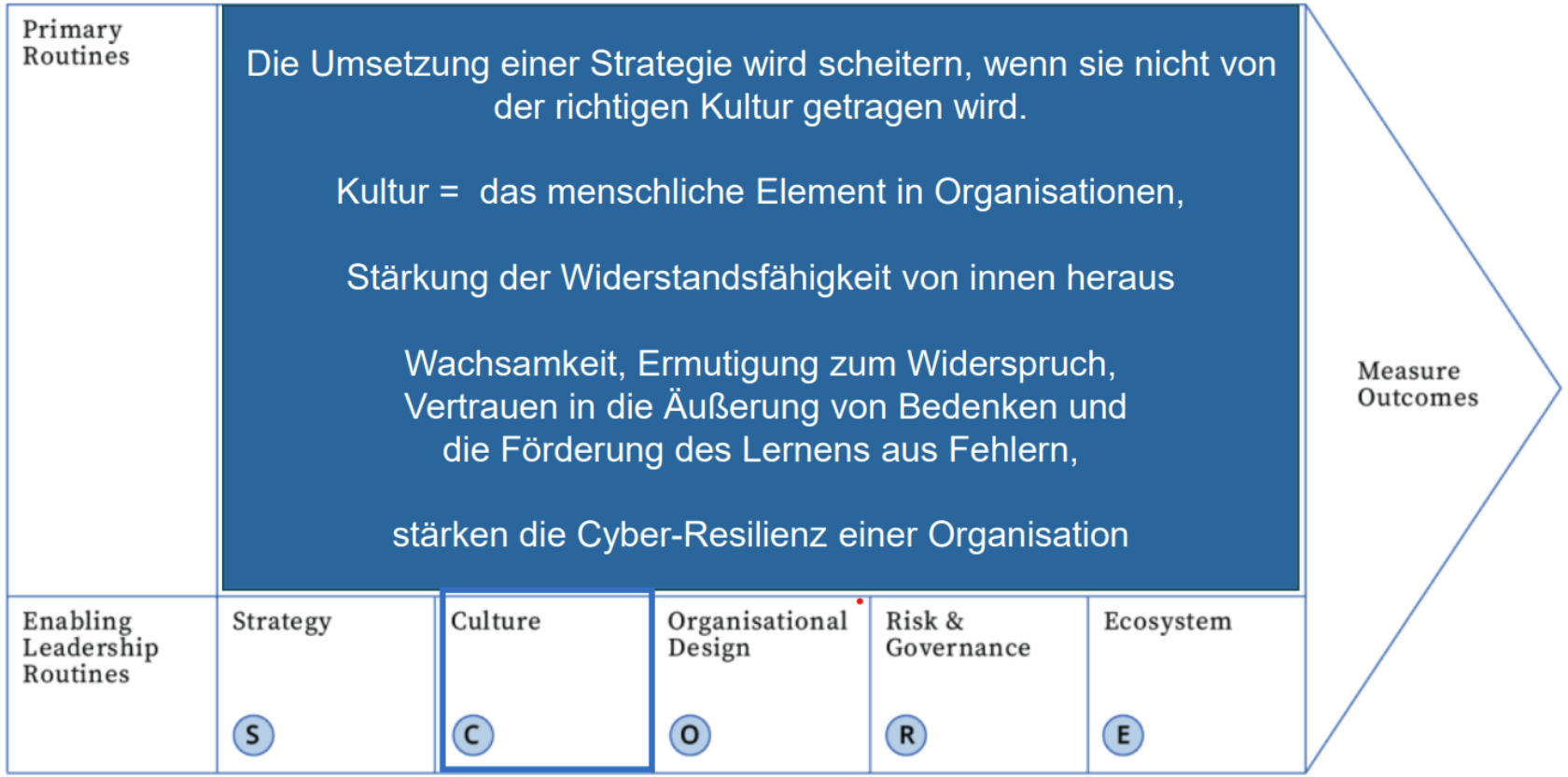


Quelle: ISTARI –Navigatorprogramm 2023

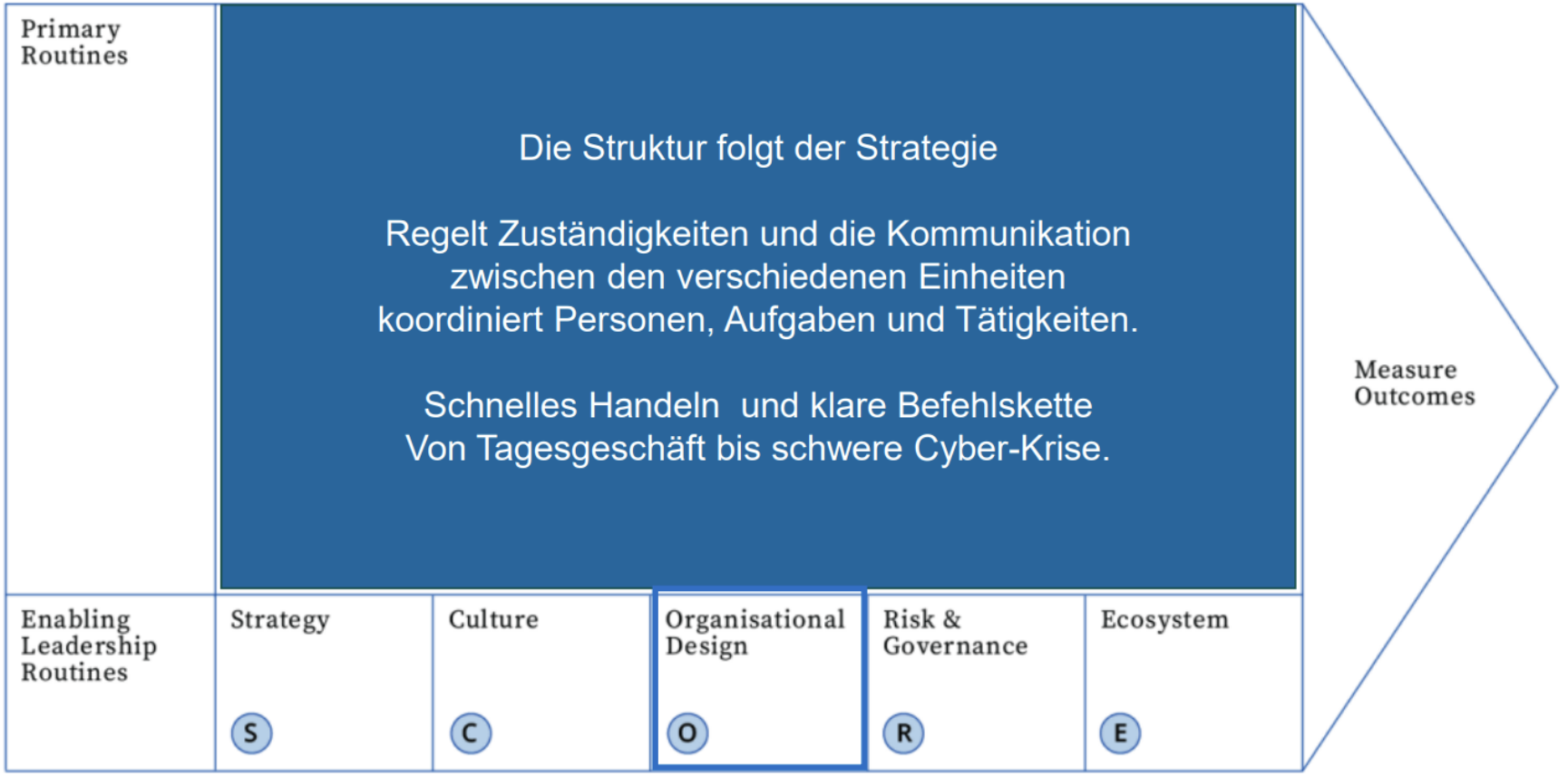
ORGANISATIONS - STRATEGIE



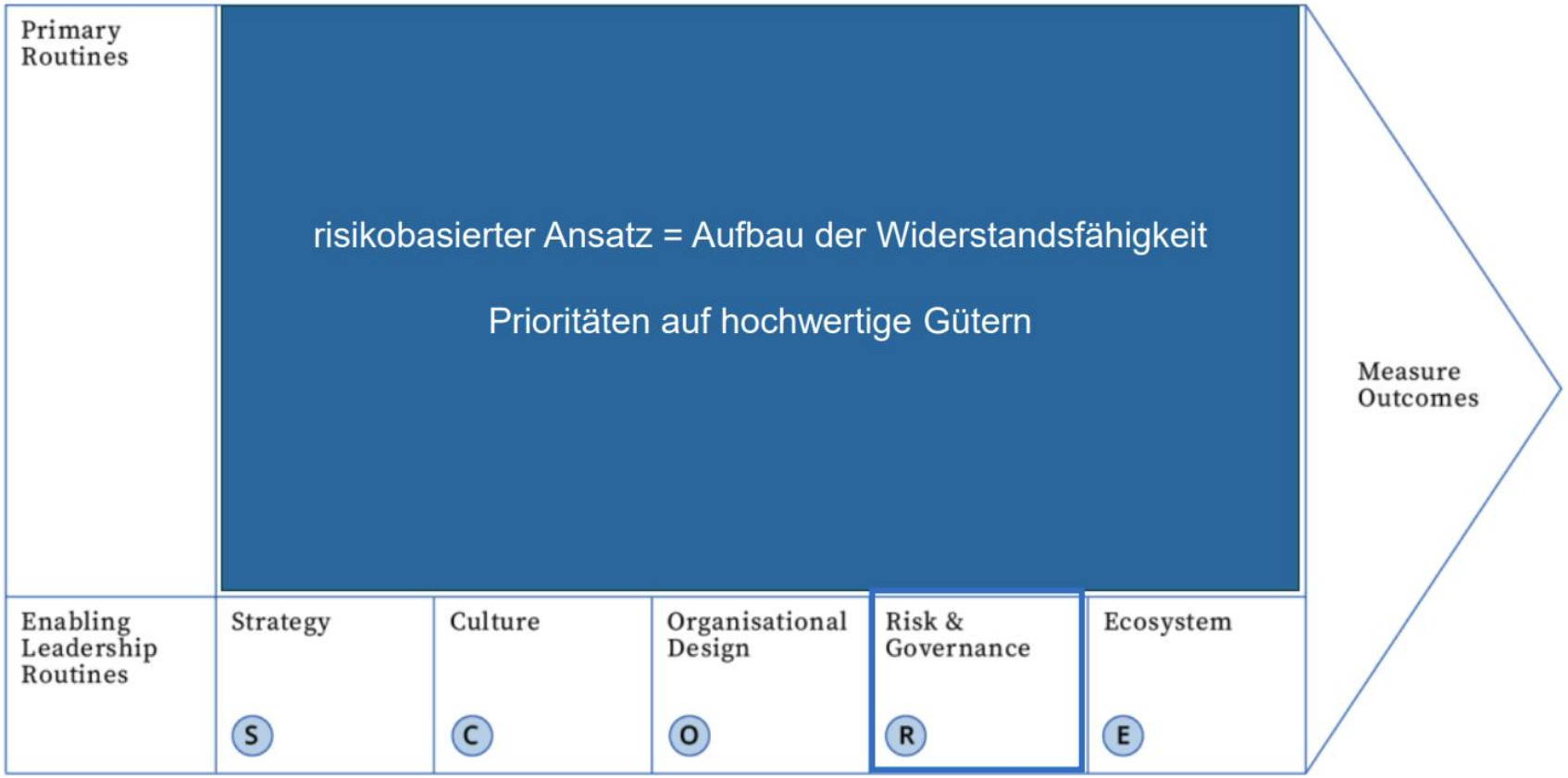
ORGANISATIONS - KULTUR



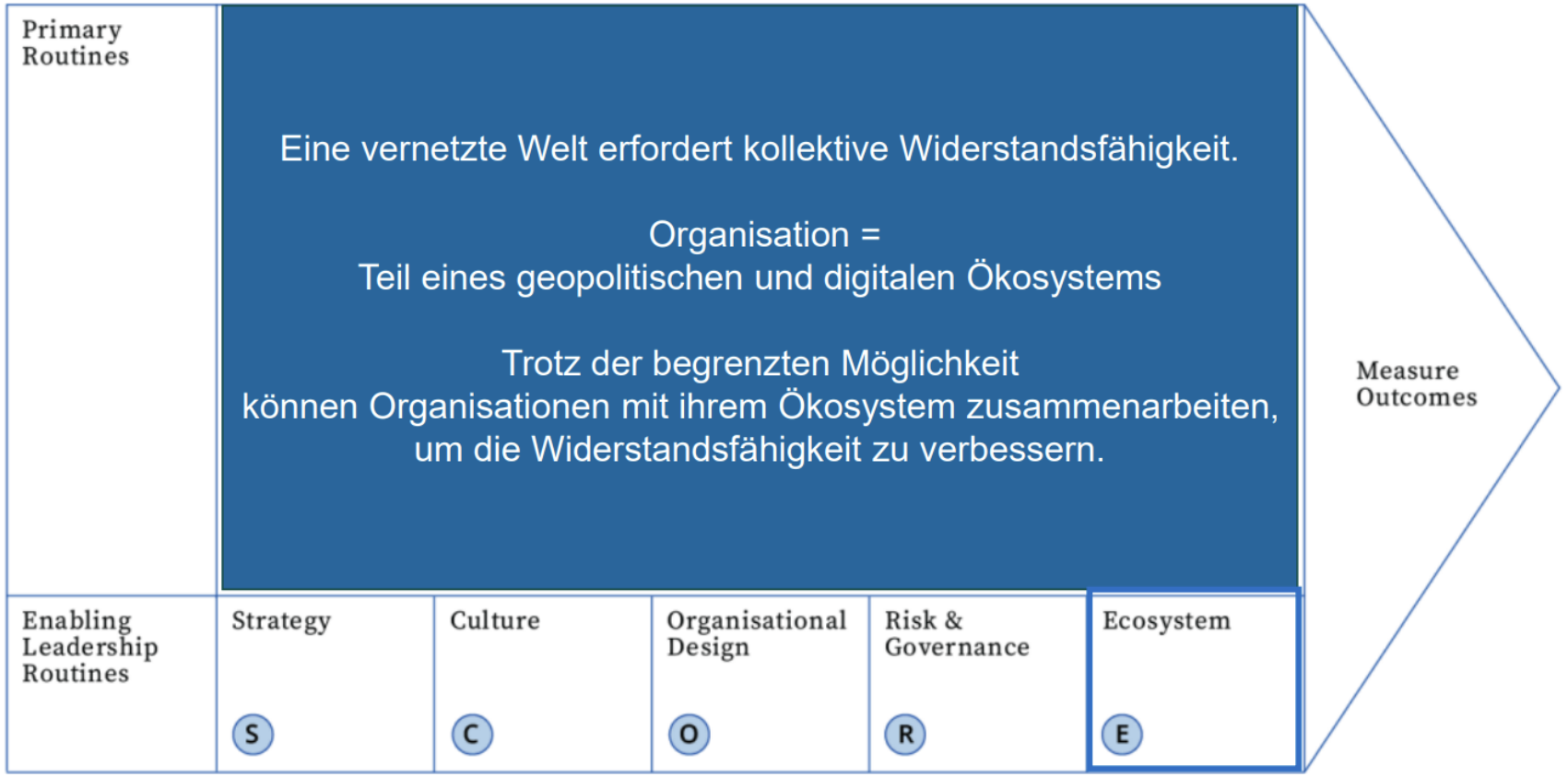
ORGANISATIONS – AUFBAU-/ABLAUF-ORGANISATION



ORGANISATIONS - RISIKOMANAGEMENT



ORGANISATIONS - EINBETTUNG IN DAS ECO-SYSTEM



GRUNDZÜGE DER IT-STRATEGIE

Die Informationstechnologie wird für die MPG immer wichtiger und ist zunehmend von entscheidender Bedeutung im wissenschaftlichen Wettbewerb.

Wachsende Anforderungen wie die Verarbeitung großer Datenmengen und der Einsatz von KI erfordern leistungsfähigere Rechenzentren, effiziente Softwaresysteme und eine IT-Infrastruktur auf Spitzenniveau.

Auch der Verwaltungsbereich steht vor der Herausforderung, komplexe gesetzliche Vorgaben effizient mit modernen IT-Lösungen umzusetzen.

Das Strategiepapier befasst sich daher intensiv mit folgenden Themenbereichen:

Wissenschaftliches Rechnen, IT-Governance, Digitalisierung in der Verwaltung, IT-Sicherheit und Rekrutierung von IT-Personal

Inhalt

Ziele der IT-Resilienz-Strategie

Schutz der Infrastruktur vor erfolgreichen Angriffen

Schutz vor unautorisierten Zugriff

Behebung erkannter Schwachstellen

Ausgeprägte Sicherheitskultur (Mensch, Prozesse, Technik)

Just Culture (Fehlerkultur)

Security-by-Default

Defense-in-Depth

Privacy-by-Default

Angriffserkennung und Systemdokumentation

Potentielle Einfallstore schließen

Hard- u. Software Inventar inkl. Cloud Updates schnell u. unkompliziert installieren

Analyse & Monitoring – Metriken

SOC

Forensik, Incident Response

Reduktion von Komplexität und Auswirkungsradien

Netzwerk-/Systemtrennung (Zero Trust)

Reduktion Gesamtkomplexität

Teams & Best Practice

MPG-Cloud vor Public Cloud

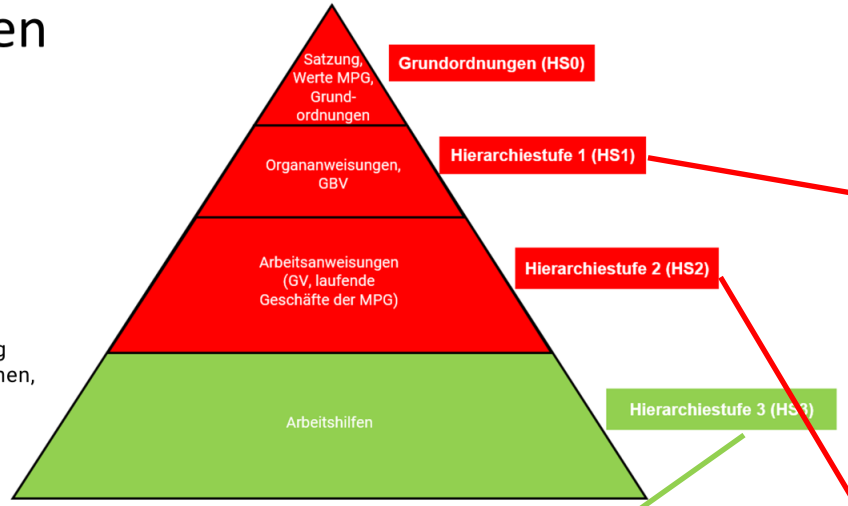
Schnelle Rückkehr zum Regelbetrieb

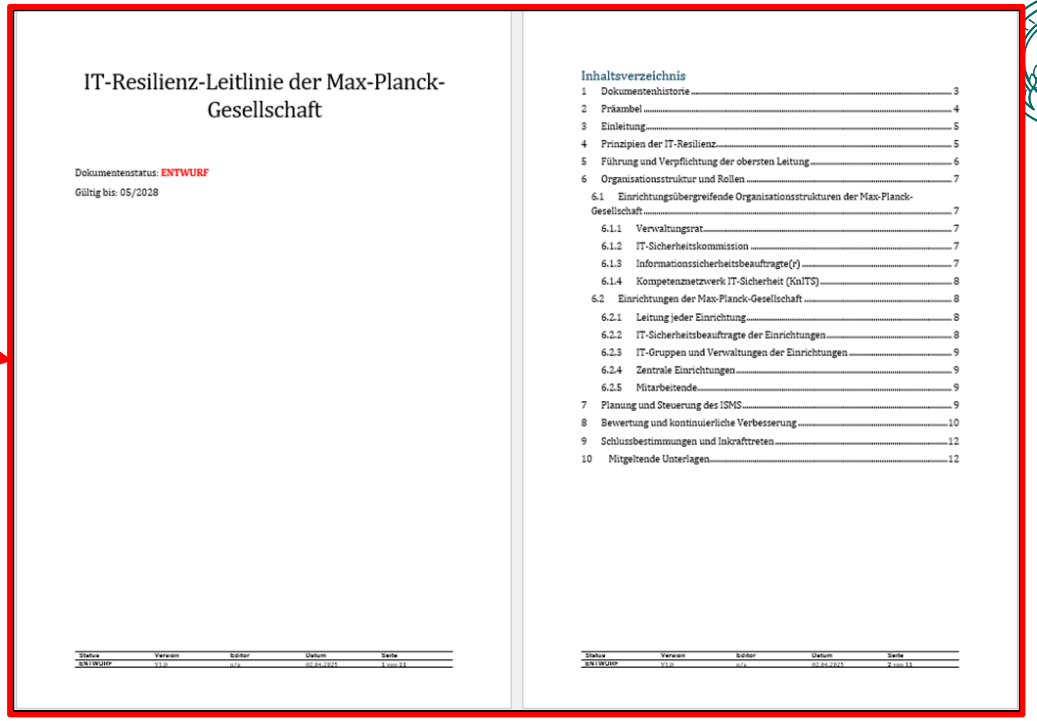
Backup- & Notfallpläne – Wiederherstellungspläne)
Training, ERT
Wiederherstellungspläne

Klare Formate – Anweisungen und Arbeitshilfen

Rot = alle verbindlichen Formate (abschließend) + Anlagen

Grün = Hilfen zur Umsetzung der Regelungen (Informationen, Empfehlungen ohne Weisungscharakter)



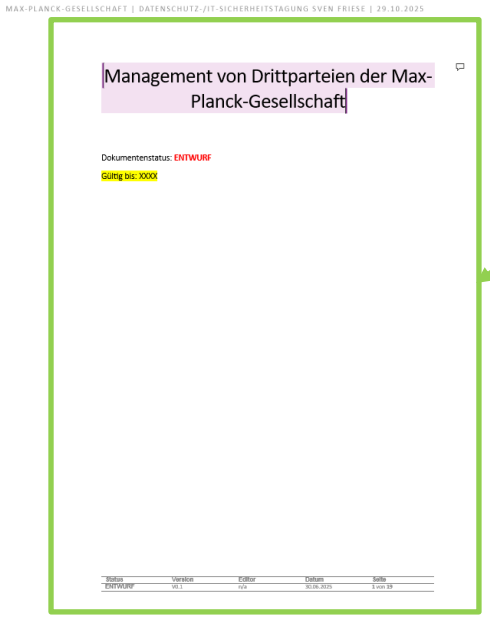


IT-Resilienz-Leitlinie der Max-Planck-Gesellschaft

Dokumentenstatus: ENTWURF

Gültig bis: 05/2028

Inhaltsverzeichnis

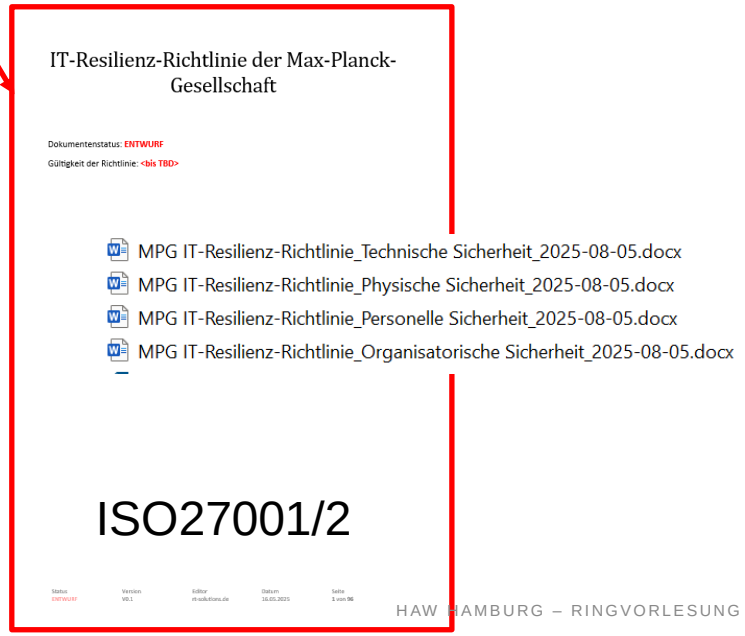


MAX-PLANCK-GESELLSCHAFT | DATENSCHUTZ-/IT-SICHERHEITSTAGUNG SVEN FRIESE | 29.10.2025

Management von Drittparteien der Max-Planck-Gesellschaft

Dokumentenstatus: ENTWURF

Gültig bis: XXXX



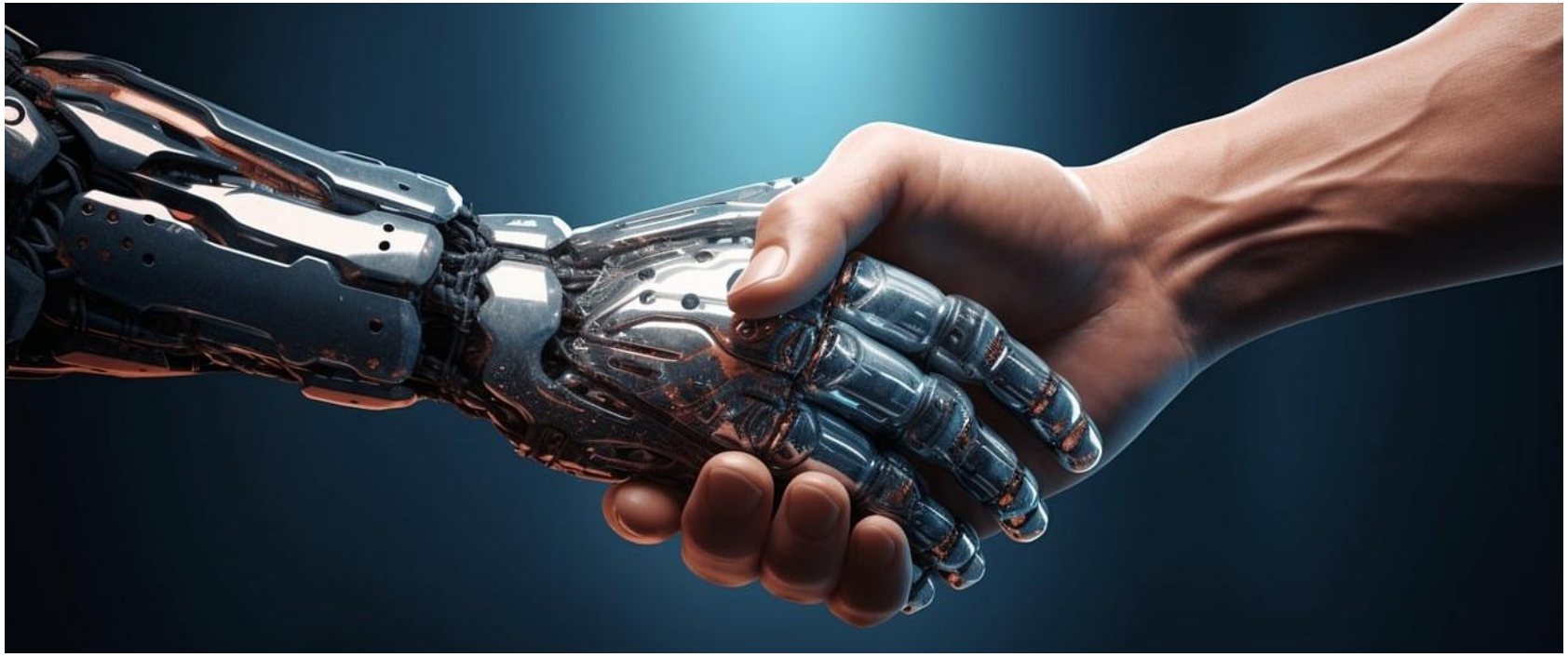
IT-Resilienz-Richtlinie der Max-Planck-Gesellschaft

Dokumentenstatus: ENTWURF

Gültigkeit der Richtlinie: <bis TBD>

- MPG IT-Resilienz-Richtlinie_Technische Sicherheit_2025-08-05.docx
- MPG IT-Resilienz-Richtlinie_Physische Sicherheit_2025-08-05.docx
- MPG IT-Resilienz-Richtlinie_Personelle Sicherheit_2025-08-05.docx
- MPG IT-Resilienz-Richtlinie_Organisatorische Sicherheit_2025-08-05.docx

ISO27001/2



Guntram Rupp
Informationssicherheitsbeauftragter

Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V.
Hofgartenstr. 8, 80539 München

Telefon + 49 89 2108-1317
E-Mail guntram.rupp@gv.mpg.de