IT-Sicherheitsmanagement - zukunftssicher und ökonomisch

33. GLT-Anwendertagung 2019

Arne P. Helemann

Portfoliomanager – Cybersecurity
TÜV Rheinland i-sec GmbH

TÜVRheinland®
Precisely Right.

Referent

Arne P. Helemann

Portfoliomanager Cybersecurity
TÜV Rheinland i-sec GmbH
Arne.helemann@i-sec.tuv.com

TÜVRheinland®
Precisely Right.

1

Topic

IT-Sicherheitsmanagement
- zukunftssicher und
ökonomisch

2

Zielsetzung

Verständnis
Austausch
Diskussion

TÜVRheinland®
Precisely Right.

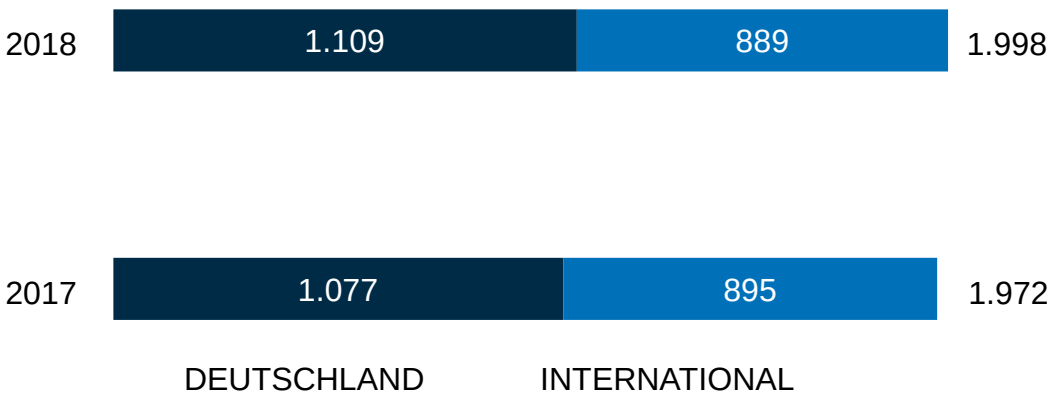
TÜV Rheinland und IT-Sicherheit?
Kurzvorstellug
TÜV Rheinland i-sec GmbH.

TÜVRheinland®
Genau. Richtig.

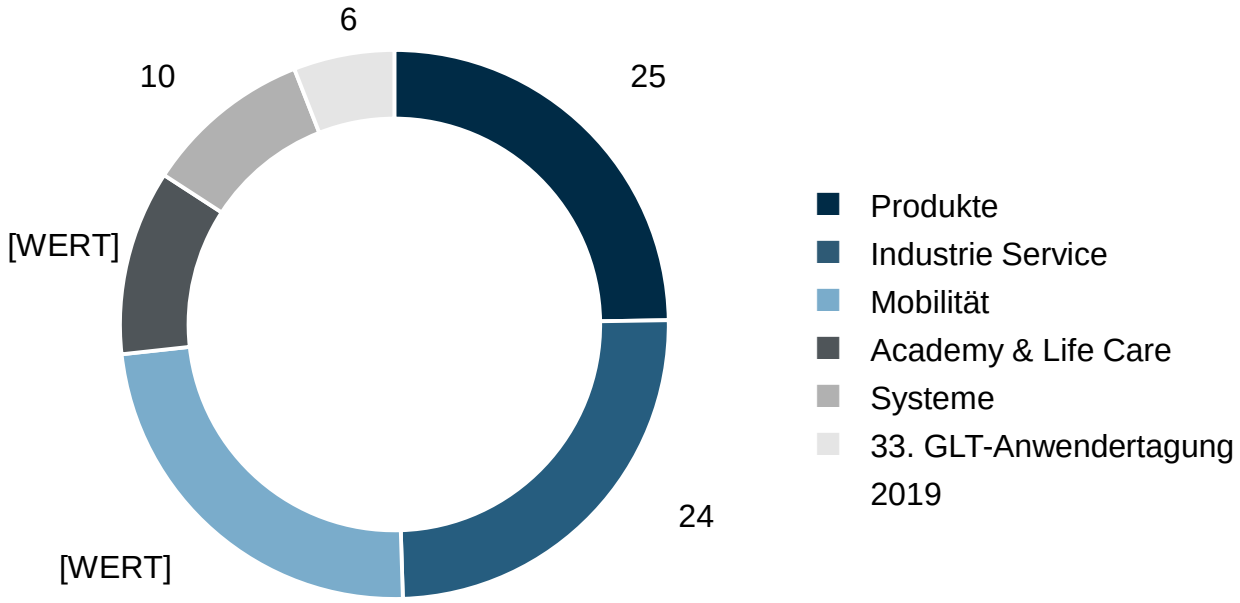
Umsatz 2018

1.998 MIO. € UMSATZ

Deutschland/International (in Millionen €)



Nach Geschäftsbereichen (in %)



Konsolidierte Daten (gemäß IFRS)

Unkonsolidierte Daten

33. GLT-Anwendertagung 2019

Eckdaten

122 MIO. € UMSATZ

6 % DES GESAMTUMSATZES

600 SPEZIALISTEN

GESCHÄFTSFELDER

- **Cybersecurity**
- **Digital Transformation**

WISSENSWERTES CYBERSECURITY

- Führender unabhängiger Dienstleister für Informationssicherheit in Deutschland
- Beratungs- und Lösungskompetenz in ganzheitlicher Informationssicherheit – von der Steuerungsebene bis ins Rechenzentrum inkl. betriebsunterstützender Leistungen
- Exzellente Technologie-Expertise, umfassendes Branchen-Know-how, strategische Partnerschaften mit Marktführern
- International zählen wir im Verbund mit unseren Schwestergesellschaften OpenSky und 2MC zu den führenden unabhängigen Anbietern

WISSENSWERTES DIGITALE TRANSFORMATION

- Wir verfügen über umfassende Expertise in allen Facetten der Digitalisierung – Smart Data, Critical Infrastructures, Connected Solutions
- Wir beraten Netzwerkbetreiber bei der Planung, beim Aufbau und bei der Pflege ihrer Telekommunikationsinfrastrukturen
- Hohe Nachhaltigkeit und Wirksamkeit durch kompetente Managementsystem-Beratung zur ganzheitlichen Unternehmensführung
- Wir unterstützen öffentliche Einrichtungen im Umfeld von Forschung und Innovation

Stand 2018: Unkonsolidierte Daten

TÜVRheinland®
Precisely Right.

TÜV Rheinland i-sec GmbH. Fakten und Zahlen.

Standorte Deutschland

- **Köln (HQ)**
- **Hallbergmoos**
- **Gelnhausen**
- **Saarbrücken**
- **Hannover**
- **Hamburg**

Fachliches Kompetenzteam

- **30 × Sales**
- **19 × Security Engineering**
- **62 × Management Beratung**
- **50 × Professional Service und Betrieb**

➔ 161 in total
Stand 01.03.2019, wachsend

Kernbranchen und Sitz unserer Kunden

- **Finanzen**
- **Automobil**
- **Energiewirtschaft**
- **Chemie/Pharma**
- **Telekommunikation**
- **Int. Mischkonzerne**
- **Transport/Logistik**
- **Öffentlicher Dienst**
- **Handel**

! Projekteinsatz an 29.000 Tagen in 2018 (+ 16% vs. Vorjahr)

TÜVRheinland®
Precisely Right.

Digital Enterprise. Protected.

Ein umfassendes, globales Serviceportfolio zum Schutz digitaler Unternehmen.

Portfolio Kategorien:

Mastering Risk & Compliance

- Governance & Strategy
- Business Continuity Management
- Risk & Compliance Management
- Data Privacy
- Information Security Management Systems

Advanced Cyber Defenses

- Identity & Access Management
- IoT Security
- Network Security
- Industrial Security
- Application Security
- Security Analytics & Detection
- Endpoint Security
- Incident Response
- Data Protection

Secure Cloud Adoption

- Cloud Security
- Enterprise Cloud Adoption
- Hybrid Infrastructure

Service Typen:

Consulting Services

Testing Services

Managed Services

TÜVRheinland®
Precisely Right.

Was ist Informationssicherheit?

TÜVRheinland®
Genau. Richtig.

Wo sind Informationen?

Informationen sind an vielen unter-schiedlichen Stellen vorhanden, z.B.

In **Netzwerken**
(z.B. Datei im Abteilungslaufwerk)

Auf **Speichermedien** (z.B. auf USB-Sticks)

Auf **mobilen Systemen**
(z.B. E-Mails auf dem Smartphone)

In **Dokumenten** (z.B. Personalakte)

Auf **Papier** (z.B. Gesprächsnotizen
oder Ausdrucke)

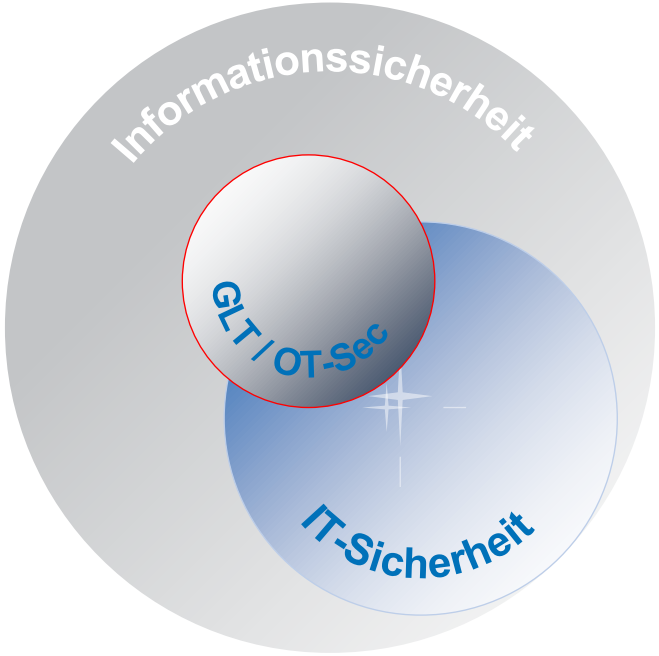
In den **Köpfen** der Mitarbeiter

TÜVRheinland®
Precisely Right.

Informationssicherheit vs. IT-Sicherheit

Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen[1]

- **Informationssicherheit beinhaltet IT-Sicherheit als Leistungsdomäne**
- **IT-Sicherheit fokussiert auf Sicherheit von IT-Systemen und darin gespeicherten Daten**
- **Informationssicherheit berücksichtigt zusätzlich weitere Themen, z.B.**
  - Strategie, Compliance, Prozesse
  - Risikomanagement
  - Personal Sicherheit, Physische Sicherheit
  - Business Continuity Management
  - Techn. und org. Maßnahmen
- **Fokus auf Schutzbedarf der Informationen**
  - Vertraulichkeit, Verfügbarkeit, Integrität



[1] (ISO/IEC 27001)

TÜVRheinland®
Precisely Right.

Anforderungen. Herausforderungen.

Keine singuläre Sicht möglich.

TÜVRheinland®
Precisely Right.

Anforderungen. IT- und Informationssicherheit.

- Exemplarisch -

Erfüllung von Anforderungen an Cybersecurity (Verträge, Regularien) **1**	Strategische Steuerung der Cybersecurity (z.B. Informations-management-system (ISMS)) **2**	Identifikation und Management kritischer Cyber-Assets **3**	Identifikation und Management von Cybersecurity Risiken **4**	Betrieb von Maßnahmen zur Angriffs-prävention und -erkennung **5**
Implementierung eines Business Continuity Management (BCM) **6**	Umsetzung branchenspezi-fischer Sicher-heitsstandards **7**	Sicherheitsaudits, Prüfungen oder Zertifizierungen **8**	Meldepflichten **9**	… **10**

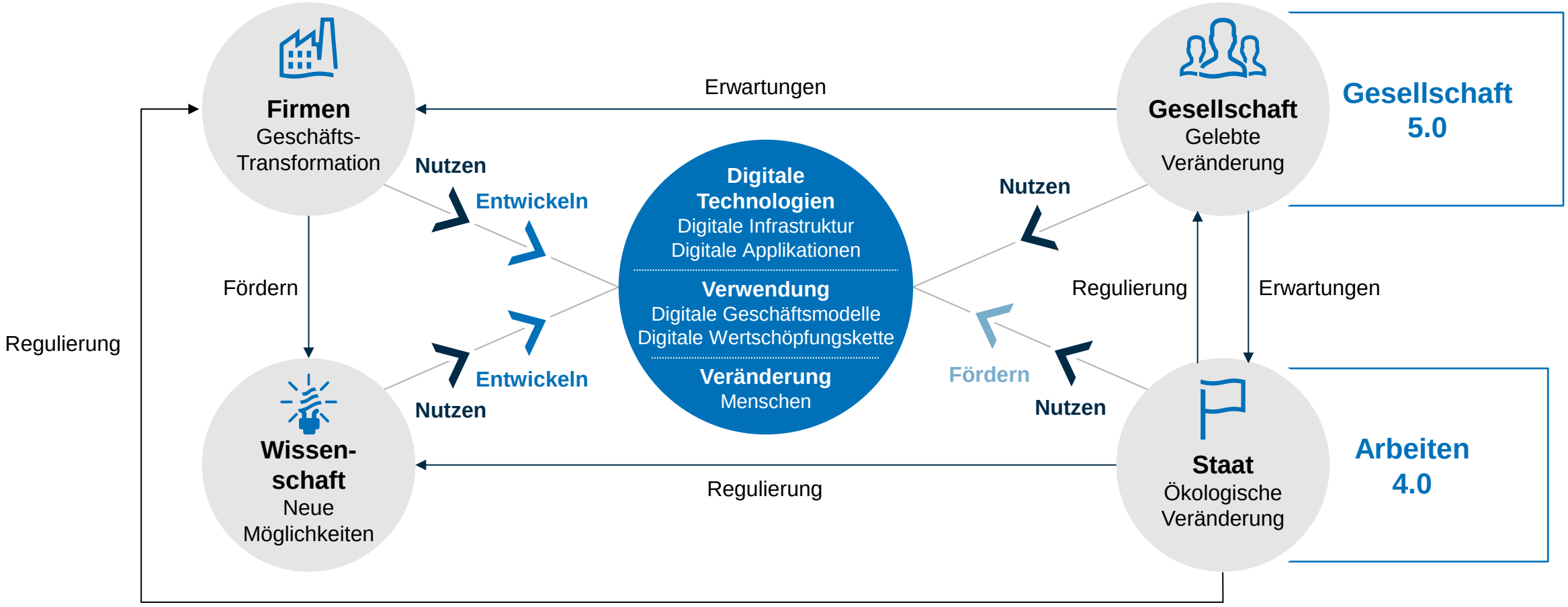
TÜVRheinland®
Precisely Right.

Was ist digitale Transformation?

TÜVRheinland®
Genau. Richtig.

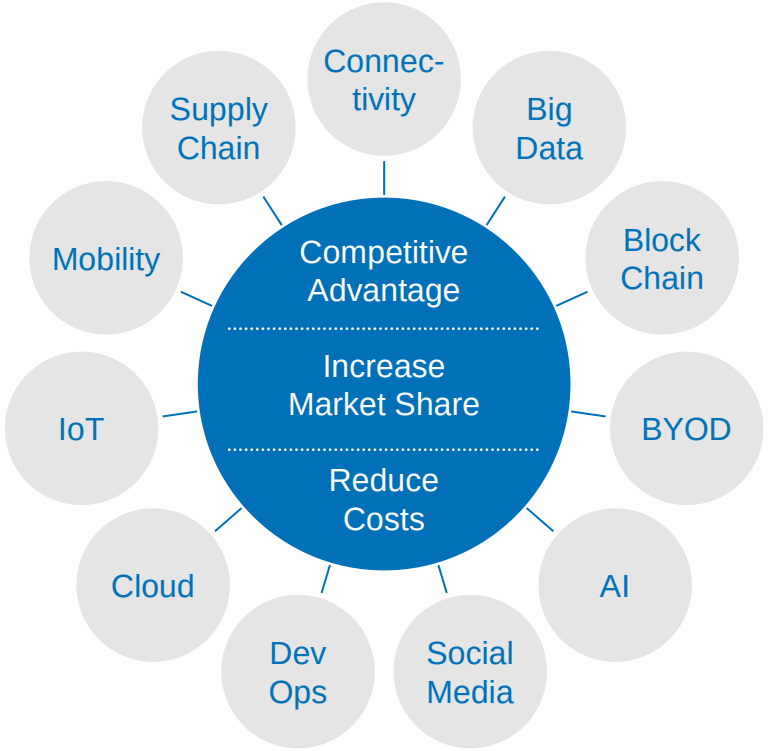
Was ist Digitale Transformation?

Es geht über Industrie 4.0 hinaus! Es betrifft die gesamte Gesellschaft!



TÜVRheinland®
Precisely Right.

Was ist “Business Transformation”?



TREIBER ODER ERFORDERLICH?

Neue Technologie & Innovation	Kontinuierliche Veränderung	Neue Kunden und Interaktion
Digitale Prozesse	Organisatorische Veränderung	Neue Partner und Interaktion
Daten getrieben	Art zu Arbeiten	Kultureller Wandel

! Digitale Transformation bedeutet vor allem kontinuierliche Veränderung, jetzt und in der Zukunft.

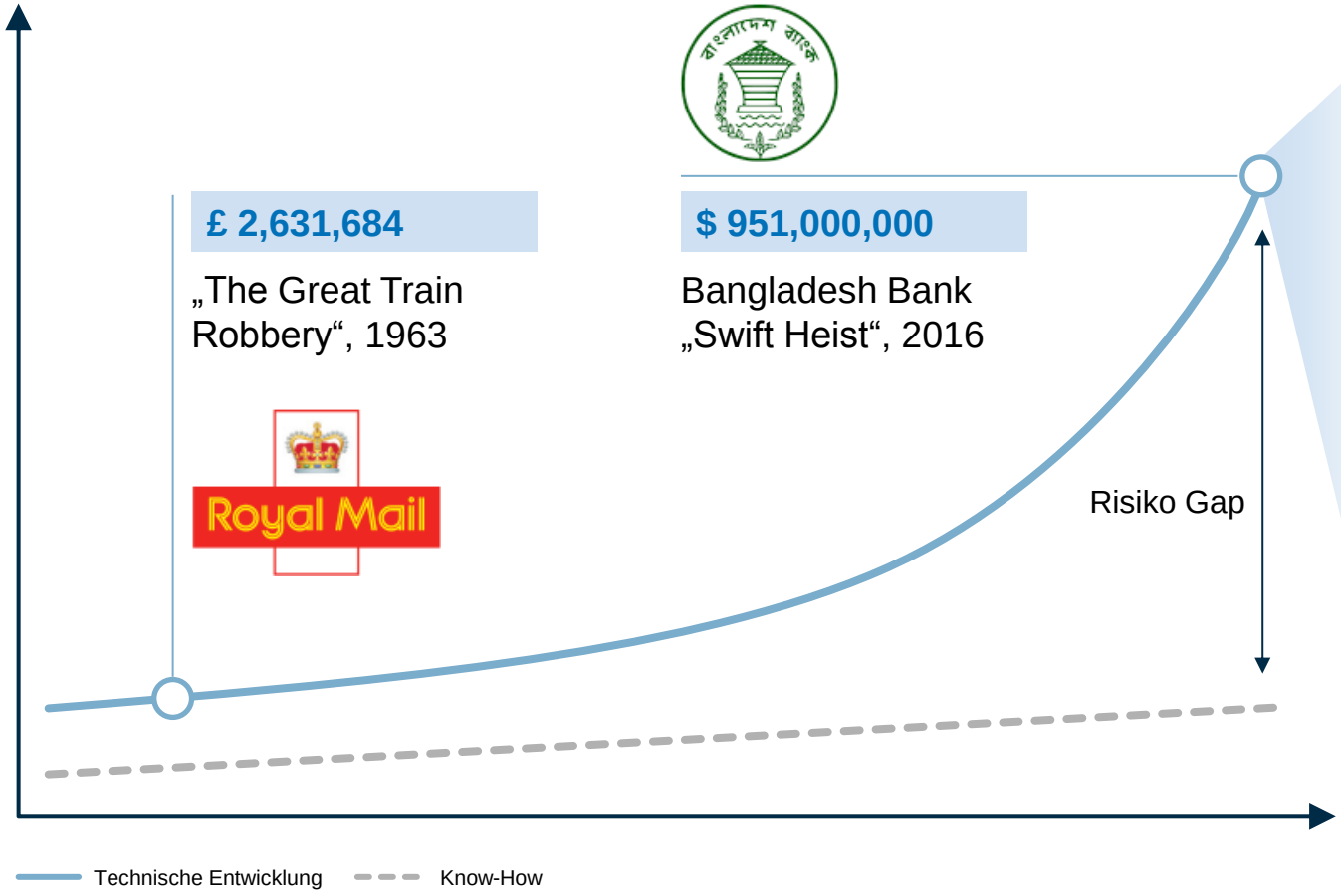
TÜVRheinland®
Precisely Right.

Cyber Risiken in der Digitalen Transformation.

TÜVRheinland®
Genau. Richtig.

Digitalisierung schreitet voran. Unaufhaltsam!

Risiken entwickeln sich auch exponentiell.



INDUSTRIE 4.0

- Automation
- Skalierbarkeit und Interkonnektivität
- AI und Machine Learning
- Agilität

CYBER RISK 4.0

- Automatisierte Attacken
- AI und Machine Learning
- Angreifer sind agil
- Komplexität erhöht Angriffsoberfläche
- Verwundbarkeit ist fast nicht zu vermeiden

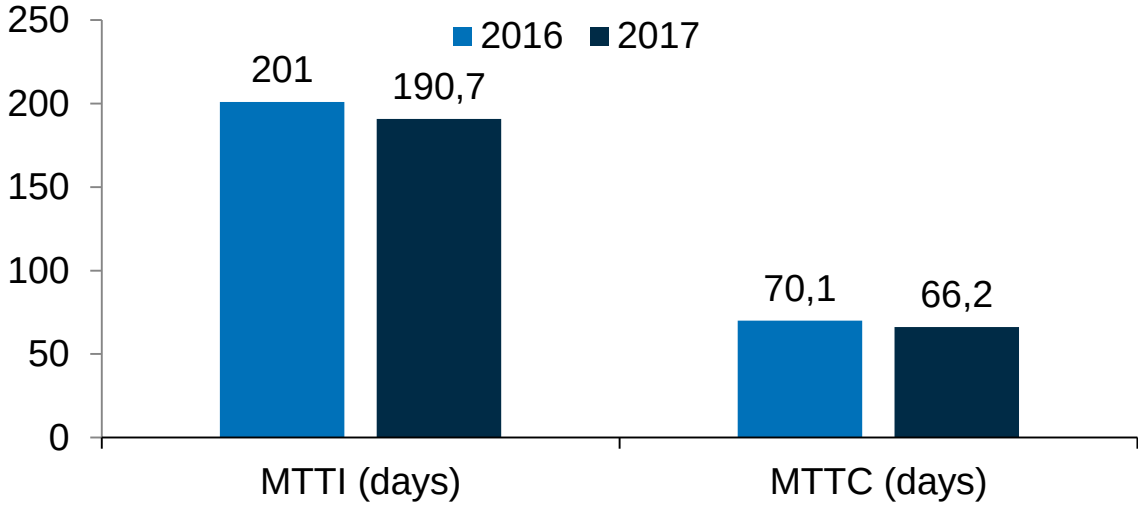
Cyber Risk = Business Risk

TÜVRheinland®
Precisely Right.

Cyber Risiken in der Digitalen Transformation

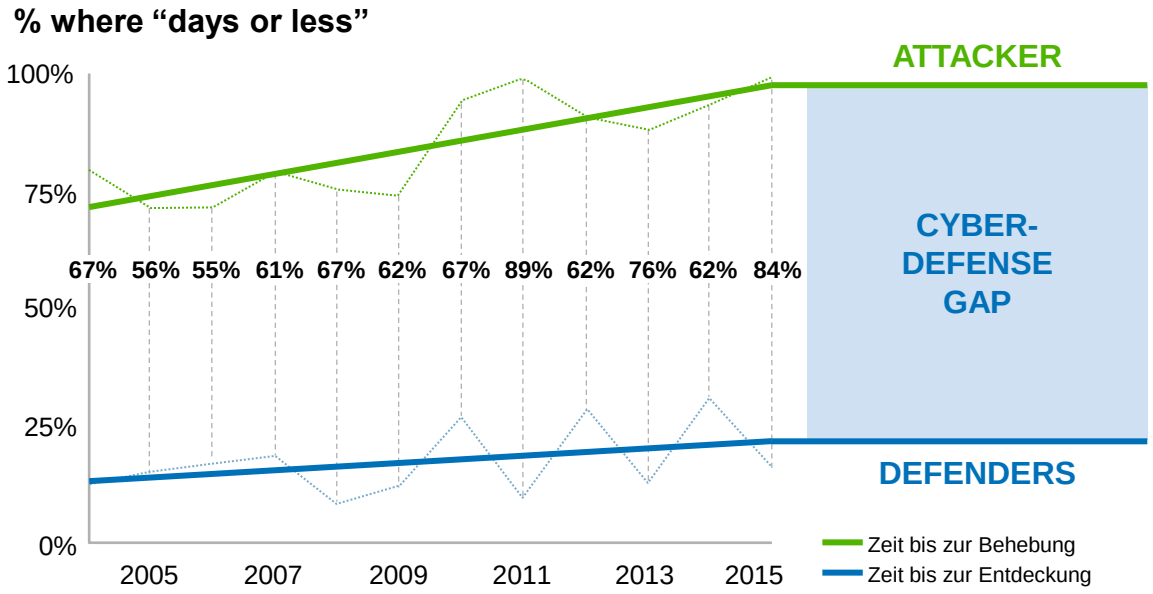
Cybersecurity als Enabler und Innovator – Innovationslücke

DIE ZEITEN UM ANGRIFFE ZU ERKENNEN UND ZU BEHEBEN VERRINGERN SICH NUR LANGSAM[2]



2017: Im Schnitt braucht es 190 Tage einen Vorfall, verursacht durch einen Angreifer zu identifizieren und weitere 66,2 Tage um diesen zu beheben.

VERTEIDIGER VERLIEREN DEN INNOVATIONS WETTKAMPF[1]



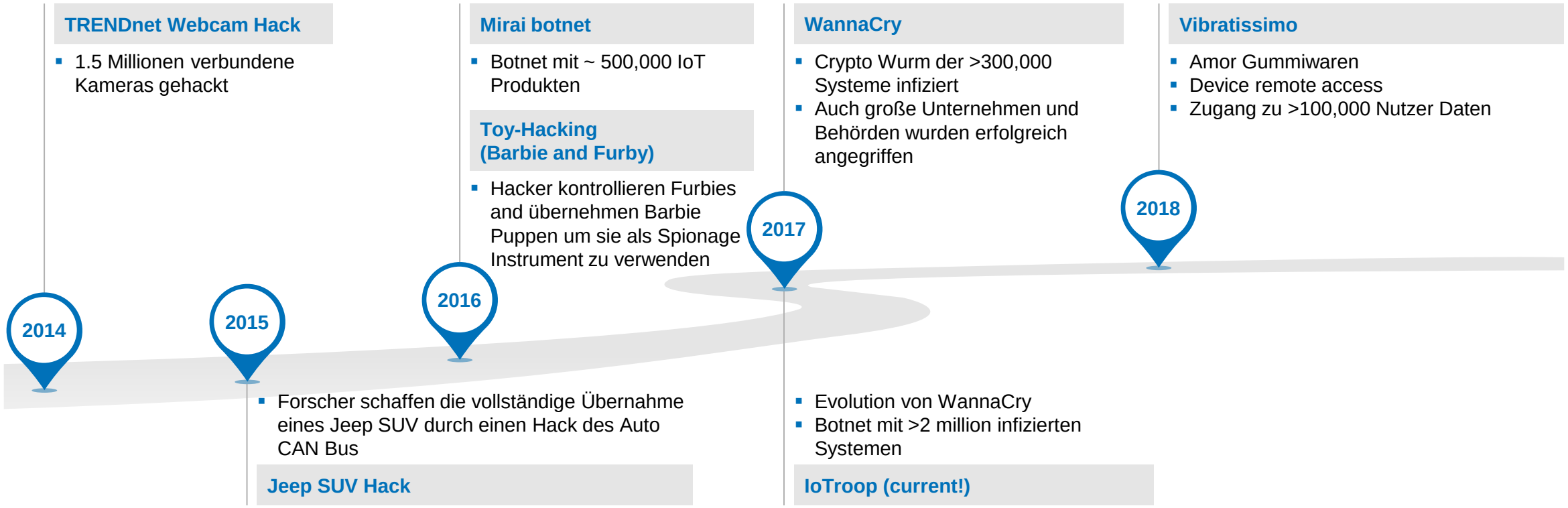
Average total cost of a data breach	Average cost per stolen record	Cost increase per record
$4.31M	**$225**	**25%**

[1] Verizon DBIR | [2] Ponemon Institute

TÜVRheinland®
Precisely Right.

Eine kurze Historie von Cyber Attacken

Kurze Auswahl an Beispielen



TÜVRheinland®
Precisely Right.

Eine kurze Historie von interessanten Attacken

22. Januar 2016, 18:22 Uhr Ukraine

Bundesamt geht von Hackerangriff auf ukrainisches Stromnetz aus

Umspannwerke fielen reihenweise aus, Hunderttausende waren ohne Strom. Für den Angriff Ende Dezember soll eine russische Hackergruppe verantwortlich sein. War es Vergeltung?

Source: securityaffairs.co, November 2018

Iran hit by a more aggressive and sophisticated Stuxnet version

November 1, 2018 By Pierluigi Paganini

Iran's strategic network was hit by a new destructive and sophisticated version of the Stuxnet cyber weapon, the Hadashot TV reports.

According to the Hadashot TV, Iran's strategic network was hit by a destructive malware-based attack hours after Israel revealed the Mossad had thwarted an Iranian murder plot in Denmark, and days after Iran's President Hassan Rouhani's phone was tapped.

Attackers used a malware similar to Stuxnet, the cyber weapon that hit the Iranian nuclear plant at Natanz in 2010 interfering with nuclear program of the Government of Teheran.

Source: securityaffairs.co, November 2018

Erpressung durch Hacker

Cyberattacke in der Keksfabrik

Hacker richten mit Cyberangriffen nach Schätzungen von Experten Schäden von Hunderten Millionen Euro an. Sichtbar werden die Attacken auf die Industrie aber selten: Den Tätern geht es um Erpressung.

Von Uli Ries

Source: spiegel.de, 17.08.2015

thyssenkrupp engineering. tomorrow. together.

Unternehmen Produkte Investoren Newsroom Karriere

Startseite > Newsroom > Cyberangriff auf thyssenkrupp

Cyberangriff auf thyssenkrupp

thyssenkrupp ist Ziel eines massiven Cyberangriffs geworden. Die WirtschaftsWoche berichtet hierüber in ihrer aktuellen Ausgabe vom 9. Dezember 2016.

Es handelte sich um einen professionellen Angriff, der nach unseren Informationen einer Angreifergruppe im südostasiatischen Raum zugeordnet werden kann. Nach unseren

Kontakt

Robin Zimmermann

Source: thyssenkrupp.com, 2016

Wenn Cyberkriminelle ein Krankenhaus lahmlegen

Nach einem Hackerangriff verwenden Chefärzte Klemmbretter statt iPads, Arztbriefe werden wieder per Hand geschrieben. Ein Besuch im Klinikum Neuss.

Source: sueddeutsche.de, 20.03.2016

Allianz

Home Services Sectors Claims Global Offices News Insights

Global Risk Dialogue
Expert Risk Articles
Marketing Brochures
Reports
Videos
Events
AGCS Newsletter
Podcasts

Expert Risk Articles

Print Share

The "Internet of Things" and piracy increasing cyber exposures

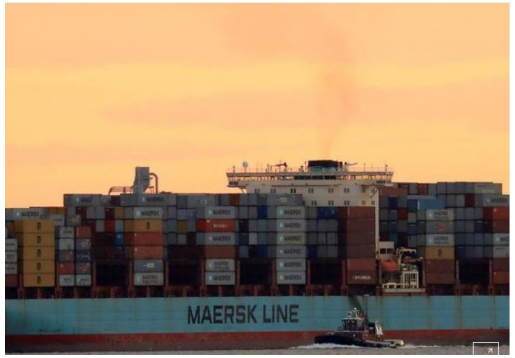
Cyber incidents in the maritime industry continue to threaten and will intensify as a result of "the internet of things" and increased digitalization. Maritime organizations recognize the importance of guidelines to inform and protect increasingly vulnerable shippers. Meanwhile, piracy incidents are not abating, with pirates targetting holes in cyber security to identify specific cargoes.

Source: allianz.de, Feb. 2018

Global shipping feels fallout from Maersk cyber attack

Jonathan Saul 8 MIN READ

LONDON (Reuters) - Global shipping is still feeling the effects of a cyber attack that hit A.P. Moller-Maersk (MAERSKb.CO) two days ago, showing the scale of the damage a computer virus can unleash on the technology dependent and inter-connected industry.



Source: reuters.com, June 2017

Fiat Chrysler recalls 1.4 million cars after Jeep hack

Source: BBC.com, 2015

TÜVRheinland®
Precisely Right.

Werde ich Ziel von Angriffen?

Beispiele für das WARUM und das WIE

„Lasst die Ausländer ihre Kühe auf unsere Weiden stellen – melken werden wir sie!“

Deng Xiaoping; ehemaliger Chinesischer Ministerpräsident

„Geheimdienste müssen einheimische Unternehmen im Ausland unterstützen. (...) So sollten der SWR und andere russische Geheimdienste ihr technisches und intellektuelles Potential aktiver einsetzen."

Haupangriffsziel sind nicht die DAX 30 Konzerne sondern **kleine und mittelständische** Unternehmen.

Cyber Crime

Erpressung, Kryptierung, Bedrohung, Darknet-Baukästen

Hybride Kriegsführung

Schadensmaximierung, Reaktionsverhinderung, Verzögerung, Politische Einflussnahme

Source: www.theintercept.com/ 2018

Wirtschaftsspionage/-sabotage

Staatlich gelenkte oder gestützte Nachrichtendienste fremder Staaten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben oder ihrer Produktionsanlagen

Industriespionage/-sabotage

Ausforschung oder Sabotage eines Unternehmens durch einen Wettbewerber

Source: Landesverfassungschutz NRW 2018

TÜVRheinland®
Precisely Right.

Gefahren. Angriffsvektoren.

Beispiele aus der Praxis

Diebstahl von:
Daten (z.B. Kreditkarten, Konstruktionsdaten), Identitäten, Equipment

Ausnutzen von Sicherheitslücken, über die Angreifer Informationen abgreifen können
Schadsoftware, ungezielte Angriffe

Sehr viele Informationen werden mittlerweile online übertragen und in der Cloud/auf fremden Servern gespeichert

Informationsbeschaffung über die „Schwachstelle“ Mensch anhand psychologischer Tricks („Trickbetrug“)

Diebstahl, Betrug

IT Netzwerke, Client-Server Umgebungen

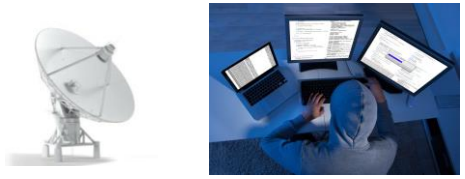
Globalisierung, Internet

Social Engineering

Mitteilungsbedürfnis

Andere hören mit
- Beim „kollegialen“ Gespräch
- In öffentlichen Besprechungs-räumen (z.B. Kaffeebar in der Firma)
- Beim Telefonieren in der Bahn

Gezielte Spionage



Abhöraktionen oder Industriespionage durch Nachrichtendienste, organisierte Kriminalität, Gelegenheits-Kriminelle

Physikalische Gefährdungen (Terror, Unruhe, Verlust wichtiger Services)

Störung von Stromnetzen / Wasserwerken.
Störungen in der öffentlichen Infrastruktur.

Unwissenheit und Fehler von Mitarbeitern

Z.B. unwissentliche Ablage von vertraulichen Informationen auf einem öffentlichen Laufwerk
Fehler in der IT-Administration
Fehler in Notfallsituationen

TÜVRheinland®
Precisely Right.

GLT / OT vs. IT

TÜVRheinland®
Genau. Richtig.

IT und OT: Definition

OPERATIONAL TECHNOLOGY (OT)

“OT is **hardware** and **software** that **detects** or **causes** a **change** through the direct **monitoring** and/or **control** of **physical devices**, **processes** and **events** in the enterprise.”

Gartner, www.Gartner.Com/it-glossary/operational-technology-ot

INFORMATION TECHNOLOGY (IT)

“IT is the **hardware**, **software**, **communication** and other facilities used to **input**, **store**, **process**, **transmit** and **Output data** in whatever form.”

ISACA , www.Isaca.Org/glossary

! **Durch stetige Standardisierung und Vernetzung von OT (Protokolle & Interoperabilität umfassend) sind beide Domänen hinsichtlich Cyber Sicherheit zu betrachten!**

TÜVRheinland®
Precisely Right.

IT und OT: Unterschiede und Gemeinsamkeiten

	Information Technology	Operational Technology
Anforderungen an die Vertraulichkeit	hoch	mittel
Anforderungen an die Verfügbarkeit	mittel	Sehr hoch
Anforderungen an die Integrität	mittel	Sehr hoch
Akzeptable Ausfallzeit	Bis zu einigen Tagen (abhängig von System)	Nicht akzeptabel
Lebenszyklus eines Systems	5-10 Jahre	15-25 Jahre
Software Changes	Häufig	Selten
Risikoszenarien	Datenverlust, Datenabfluss	Zerstörung der maschinellen Ausstattung, Fehlproduktion, Verletzung von Mitarbeitern
Auswirkungen	Betriebsunterbrechnungen, Wettbewerbsnachteil, Schaden für Leib und Leben	

Nach ISACA „The Merging of Cybersecurity and Operational Technology“ 2016

! Verschiedene Perspektiven auf die gleichen Unternehmensrisiken!

TÜVRheinland®
Precisely Right.

Grundlagen IT-Sicherheitsmanagement

TÜVRheinland®
Genau. Richtig.

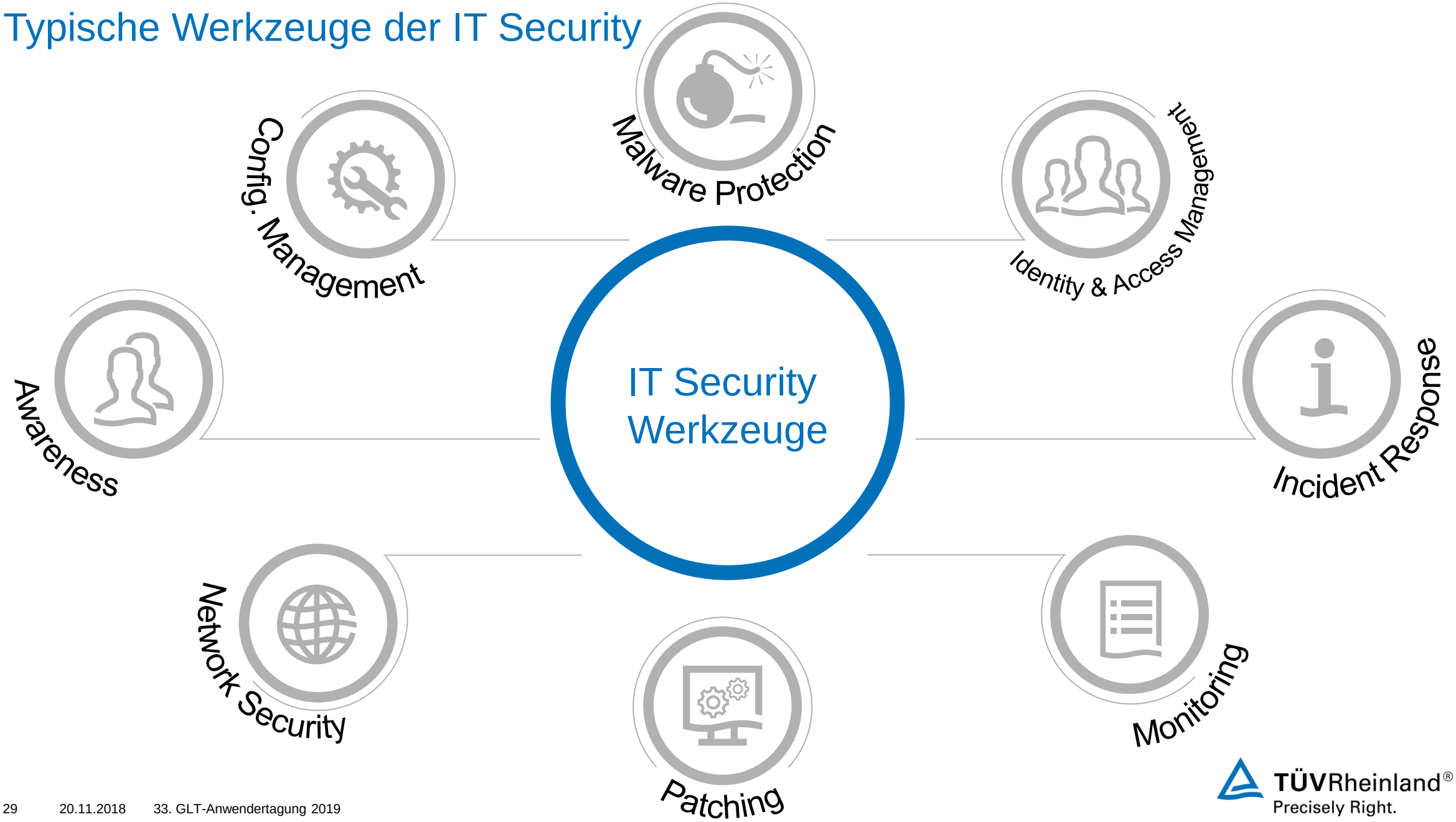
Lösung Ansatz. Gesteuerte Informationssicherheit

Strategische Ausrichtung	▪ Aufbau Informationssicherheits-Managementsystem (ISMS) - **Standards:** Z.B. ISO 27001, IT-Grundschutz, Ergänzend: Branchenstandards - **Risikomanagement:** Identifikation von Informations-Werten und Risiken ▪ Richtlinien und Standardisierung (intern) ▪ Standards und Richtlinien für den Partner und Zulieferer
Technische Maßnahmen	▪ Z.B. Segmentierung der Netzwerke ▪ Fernwartungskonzept ▪ Systemsicherheit durch Härtung ▪ Threat Management auf Perimeterebene und Endpoints
Organisatorische und Betriebliche Maßnahmen	▪ Verfahrens- und Arbeitsanweisungen ▪ Sicherheitsbewusstsein schaffen – Awareness ▪ Betriebsprozesse in Office- und Produktion synchronisieren ▪ Z.B. Berechtigungsmanagement, Patchmanagement, etc.

! **Zielsetzung: GANZHEITLICHE LÖSUNG.**

TÜVRheinland®
Precisely Right.

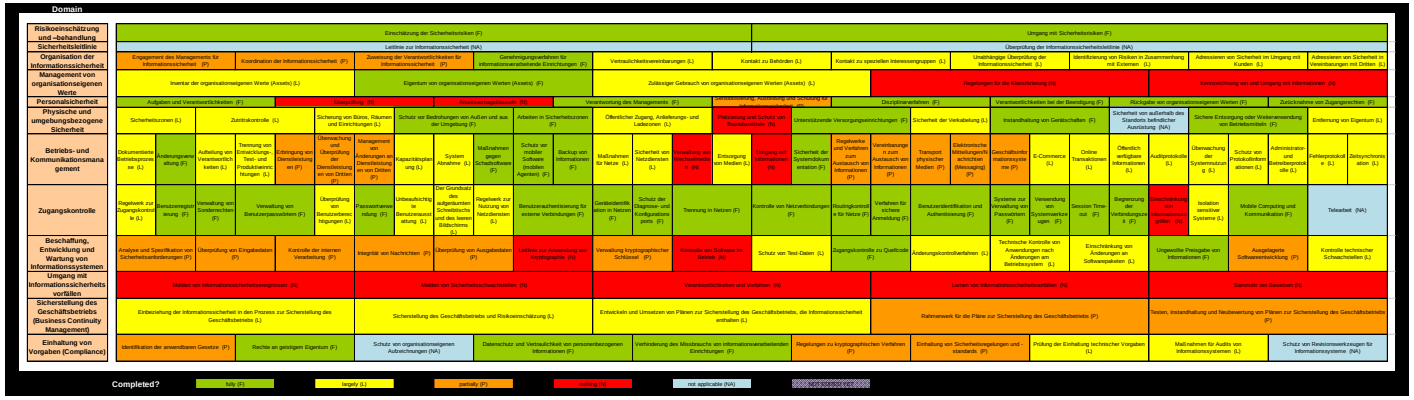
Typische Werkzeuge der IT Security



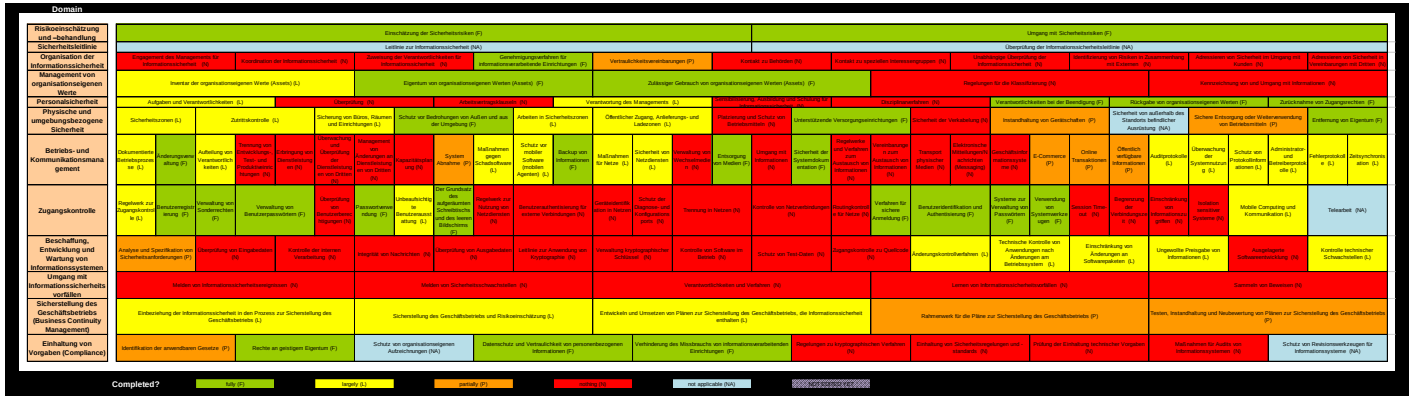
TÜVRheinland®
Precisely Right.

Heatmap. Implementierungs- und Dokumentationsgrad.

Implementierung von Maßnahmen



Dokumentation von Maßnahmen



TÜVRheinland®
Precisely Right.

Herausforderungen im Risikomanagement Ansatz

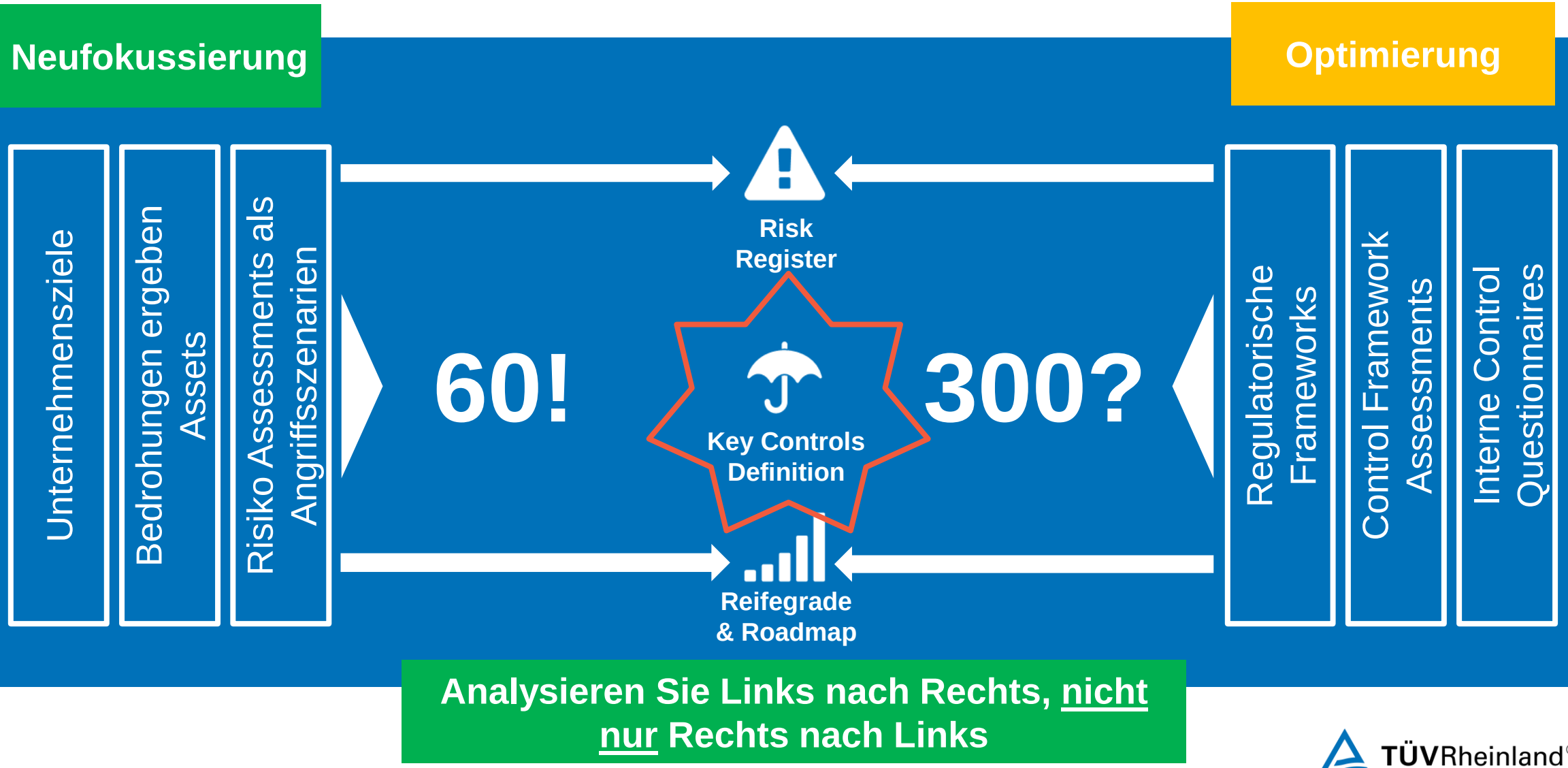
Ausrichtung des Cyber Risikomanagements an Unternehmenszielen und finanzielle Anforderungen

1	2	3	4	5
Komplexität der Organisation	**Compliance-anforderungen**	**Ineffektiver Einsatz Automatisierung**	**Angriffe werden nicht erkannt**	**Technologische Unterstützung**
Organisationen sind mit der Steuerung der Cyber Risiken überfordert, während die Bedrohungslage aufgrund des technologischen Fortschritts stetig zunimmt.	Typische Risikomanagement-ansätze basieren auf Compliance. Die regulatorischen Anforderungen sind oft „wichtiger“ als der eigentliche Angreifer.	Firmen realisieren derzeit noch nicht den potenziellen Wert von MSS und Threat Intelligence.	Szenarien, die am schwerwiegendsten für Organisationen wären, werden nicht überwacht und können so nicht erkannt werden.	Plattformen müssen Top-Down Risiken berücksichtigen und Daten aus verschiedenen Quellen aggregieren

! Top-Down Risikomanagement Techniken müssen den Fokus auf Business Context legen!

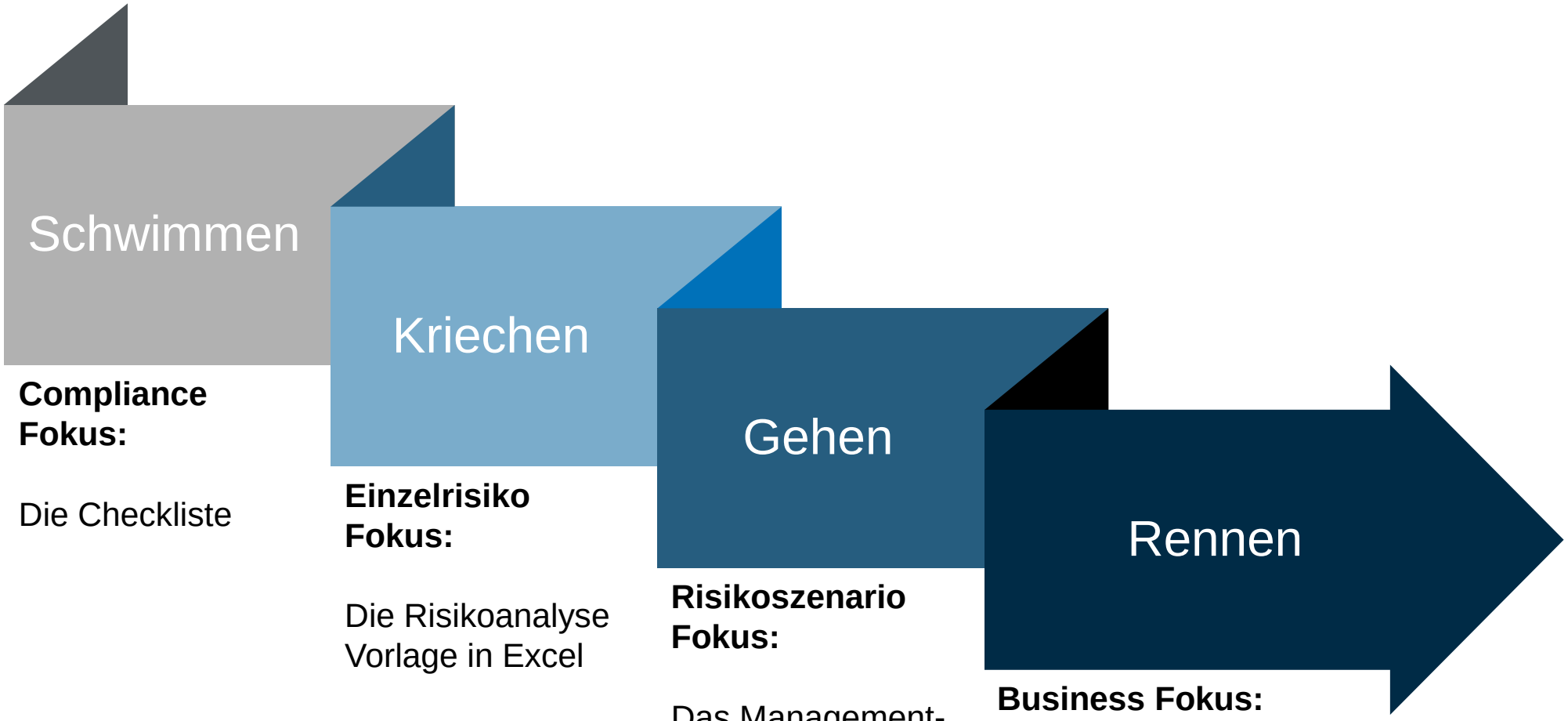
TÜVRheinland®
Precisely Right.

Neufokussierung im Cyber Sicherheitsmanagement



TÜVRheinland®
Precisely Right.

Der Evolutionäre Ansatz



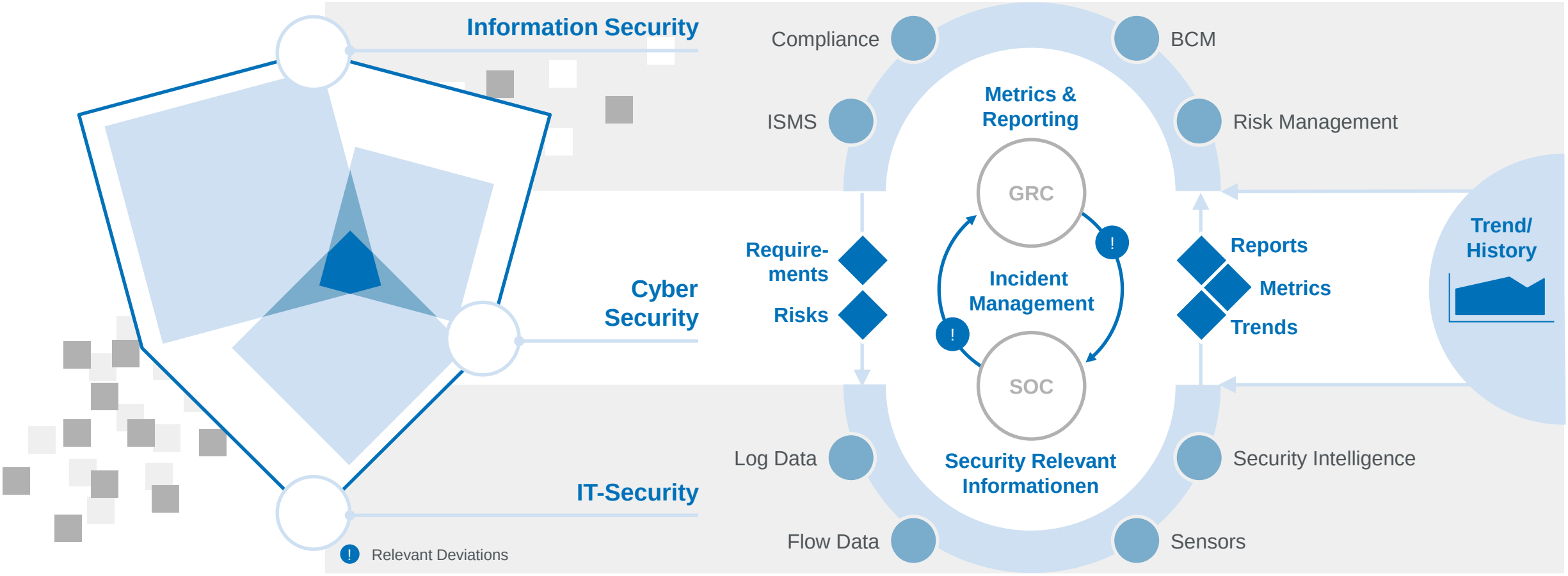
TÜVRheinland®
Precisely Right.

Der integrierte Ansatz

TÜVRheinland®
Genau. Richtig.

Cybersecurity in der Digitalen Transformation

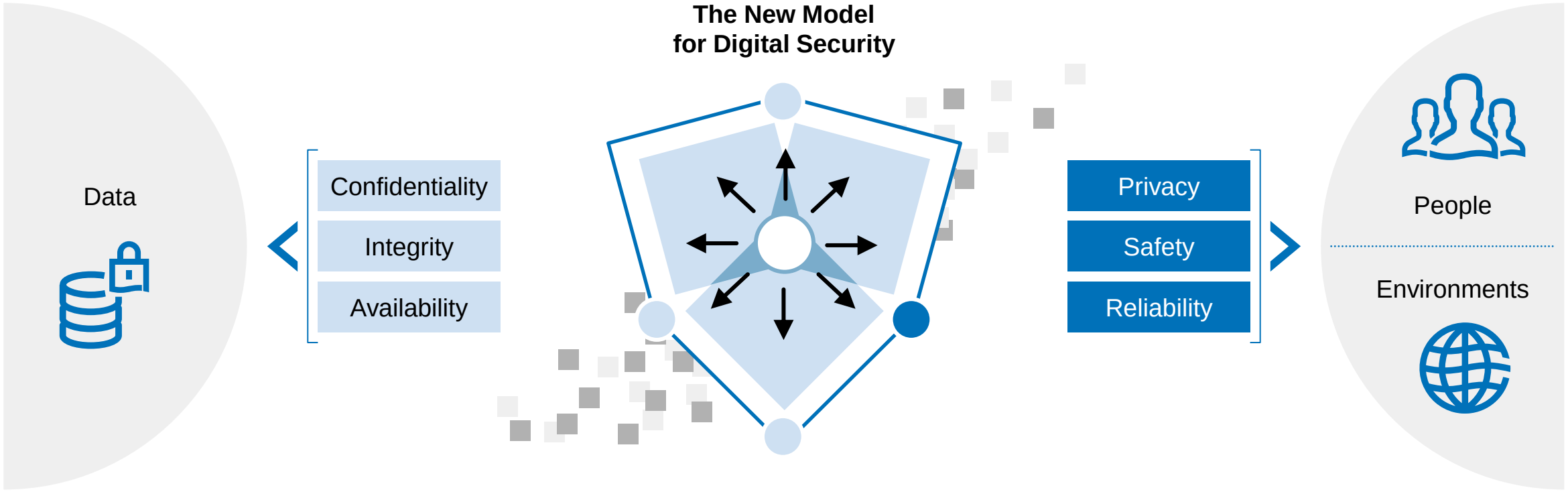
Verbinden Sie die Cybersecurity Strategy mit den Zielen der Digitalen Transformation und machen es visibel.



TÜVRheinland®
Precisely Right.

Cybersecurity in der Digitalen Transformation

SAFETY, RELIABILITY UND PRIVACY: DIGITAL SECURITY IMPERATIVES

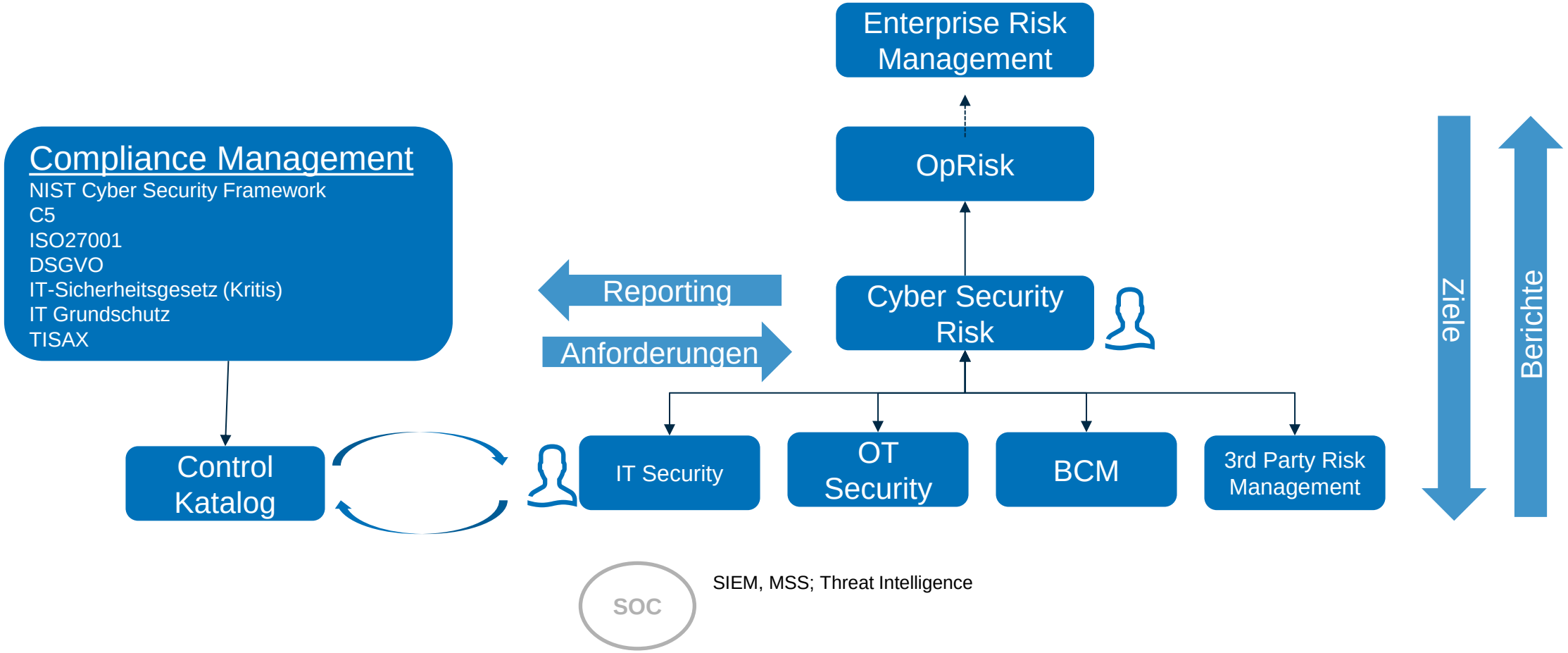


Source: Gartner Security & Risk Management Summit: „Tutorial: Gartner Essentials: Top Cybersecurity Trends for 2016 – 2017"; Earl Perkins, 12 – 13 Sept. 2016

TÜVRheinland®
Precisely Right.

Integriertes Risikomanagement Framework für Cybersecurity

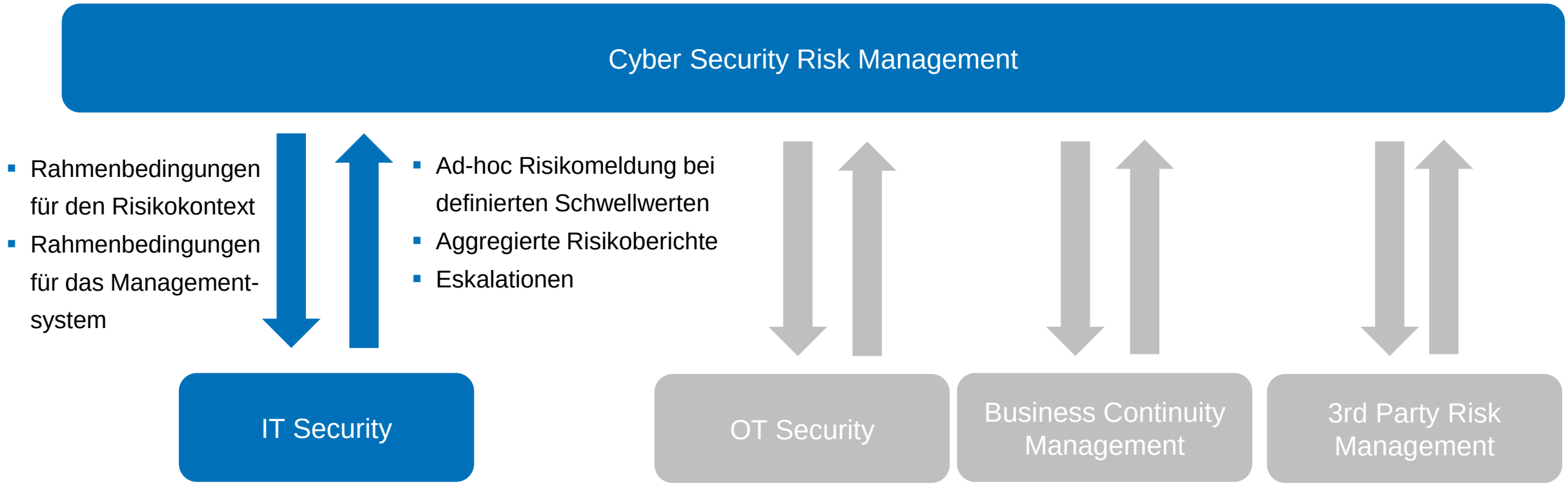
Ein schematischer Überblick.



TÜVRheinland®
Precisely Right.

Integriertes Risikomanagement Framework für Cyber Security

Schnittstelle IT Security – Cyber Security



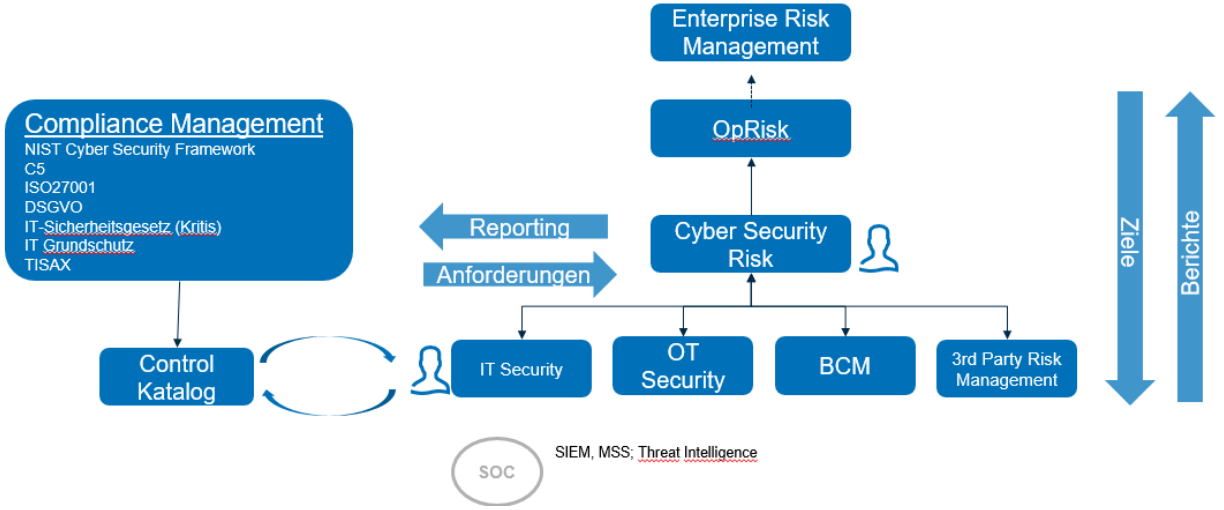
- Integration von Managed Security Services Quellen (Security Operations Center; SOC) zur (semi-) automatisierten Identifikation von Risiken (u.a. durch Threat Management)

TÜVRheinland®
Precisely Right.

Integriertes Risikomanagement Framework für Cyber Security

Vorteile der Integration von der Themenbereiche

- **Reduktion laufender Kosten** durch den Wegfall redundanter Prozesse und Ressourcen
- **Bessere Steuerung und Kontrolle** in verteilten Umgebungen
- **Kontinuierlicher Risikomanagement Prozess** statt verschiedene Zyklen in verschiedenen Domänen
- **Konsistente Darstellung von Risiken** über die Domänen => Risikotransparenz
- **Vereinfachte Einhaltung von Compliance** Vorschriften (z.B. KRITIS, HIPAA)
- **Höhere Betriebssicherheit**:
  - Weniger Gefahr für Leib und Leben
  - Weniger Betriebsunterbrechungen



TÜVRheinland®
Precisely Right.

Handlungsfelder der Cybersecurity

Grundlagen schaffen. Priorisieren. Kontinuierlich verbessern.

1 Governance & Strategien

Cybersecurity als **Business Enabler** positionieren

Umgang mit Komplexität und vernetztes Denken in den Mittelpunkt stellen

Unternehmensziele aufgreifen und auf den Bereich der Cybersecurity herunterbrechen

Best Practise in Form international anerkannter Frameworks für Informationssicherheit und Cybersecurity anwenden

2 Strukturen & Organisation

Silostrukturen, -denken und -handeln abbauen

Klassische Handlungsfelder der Sicherheit (IT, physikalische Sicherheit, IS, Compliance-Funktionen) gesamthaft betrachten und smart koppeln

In Wirkungsketten denken und die Organisation der Cybersecurity daran orientieren

3 Risiko-, Compliance- & Cybersecurity-Mgmt.

Auf- und Ausbau eines durchgängigen Risikomanagements, das operationelle Risiken der Digitalisierung vom ersten use case bis zum Regelbetrieb umfassend und dauerhaft betrachtet = Cyberrisiko-Management

Vorgaben der Regulierer als Hilfestellung nutzen

Ausbau eines Informationssicherheits-Managementsystems (ISMS) zu einem Cybersecurity-Managementsystem (CSMS)

4 Technologien & Werkzeuge

Plattform-Lösungen müssen den Vorrang erhalten; Einzellösungen und Excel-Artwork führen i.d.R. zu mehr Komplexität

Das Potential von cloudbasierten Security-Lösungen ausnutzen: Echtzeit-Sicherheitsanalysen, Detektion von Anomalien mit Hilfe von KI u.ä.

Managed Security Services nutzen: Continous Monitoring, Incident Response Advisory Services, Threat Intelligence und Security Data Analytics

5 Mitarbeiter & ihre Fähigkeiten

Mitarbeiter sind die „very first line of defence“ – Schulung und Sensibilisierung im Hinblick auf alle Gefahren des Einsatzes von alten und neuen Technologien ist eine Daueraufgabe

Kompetente und fähige Mitarbeiter werden zu einem knappen Gut und damit zu einem kritischen Erfolgsfaktor in jedem Unternehmen – neue Wege in der Personalentwicklung werden erforderlich.

! Cybersecurity 4.0: die Handlungsfelder müssen ebenfalls eine exponentielle Wirkung entfalten.

TÜVRheinland®
Precisely Right.

Zusammenfassung. Schlüsselthemen.

Digitale Transformation hört nie auf sich zu wandeln. Ebensowenig sollte es Cybersecurity.

Cybersecurity gehört in die Digitale Transformations Strategiey und es bedarf Management Unterstützung

Denken Sie darüber nach schneller UND sicherer als Wettbewerber zu sein.

Hören Sie auf verteidigungs-fokussiert zu denken, dieser Ansatz wird durch Angst verkauft.

Verstehen Sie Cybersecurity als Enabler für Innovationen und Beschleuniger für ihr Geschäft.

Cybersecurity ist das Rückgrat für die Digitale Transformation.

Kultureller Wandel ist erforderlich um Innovationen in der Cybersecurity zu ermöglichen.

"Das Ganze ist mehr als die Summe seiner Teile.“[1]

1 verkürztes Zitat von Aristoteles

TÜVRheinland®
Precisely Right.

Vielen Dank für Ihre Aufmerksamkeit.

Diskussion / Fragen

Arne P. Helemann

Portfoliomanager – Cybersecurity

Phone +49 174 1880256

Mail arne.Helemann@i-sec.tuv.com

https://tuv.com/informationssicherheit

LEGAL DISCLAIMER
This document remains the property of TÜV Rheinland. It is supplied in confidence solely for information purposes for the recipient. Neither this document nor any information or data contained therein may be used for any other purposes, or duplicated or disclosed in whole or in part, to any third party, without the prior written authorization by TÜV Rheinland. This document is not complete without a verbal explanation (presentation) of the content.
TÜV Rheinland AG

TÜVRheinland®
Precisely Right.