T.I.S.P./T.P.S.S.E. Community Meeting 2025

Berlin, 04. - 05.11.2025

Harmonisierung von Risikomanagement-Disziplinen in komplexeren Organisationsstrukturen

Patrick Hesse, EnBW

Katharina Otto, EnBW

Agenda

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

1 Ausgangslage

2 Motivation und Zielbild

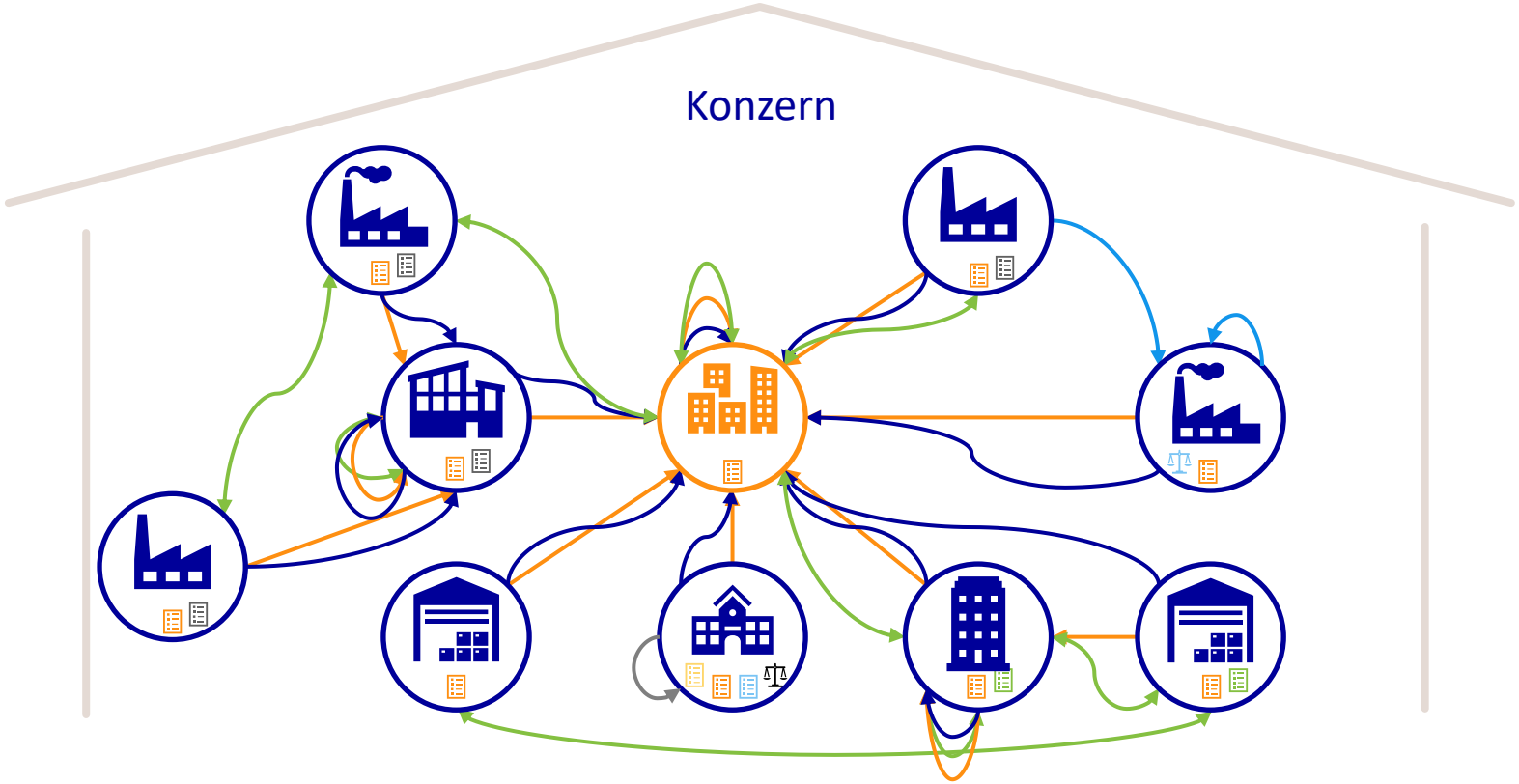
3 Kernelemente der Methodik

4 Mögliche Stolpersteine und kritische Erfolgsfaktoren

5 Mehrwert

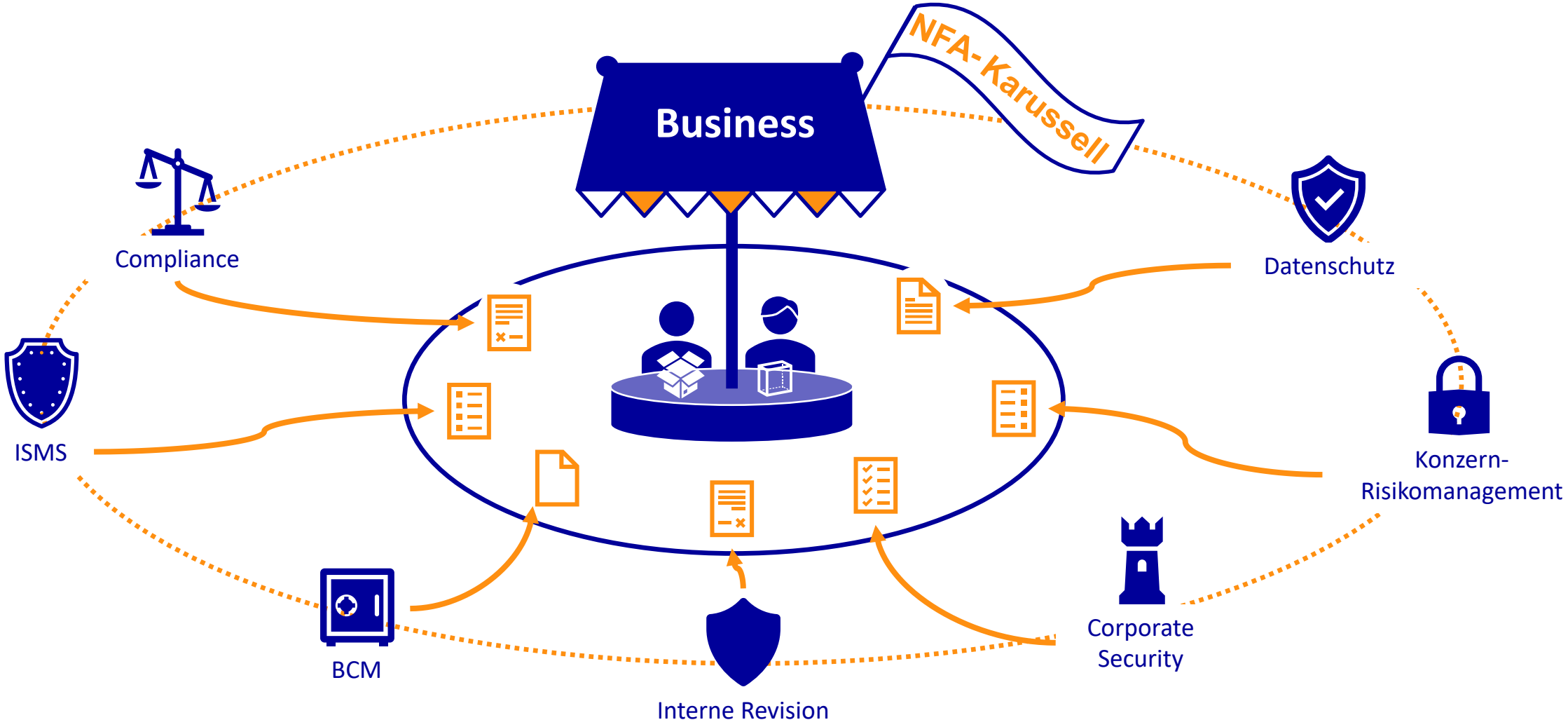
6 Fragen

Ausgangslage – komplexe Konzernstruktur



Komplexer Konzern mit **vielschichtigen Risikomanagement-** und -**Reporting-Ebenen**:
(Konzern-) Risikomanagement, Informationssicherheit, Corporate Security, Datenschutz, BCM, etc.

Ausgangslage – Compliance und NFA



Ausgangslage – Kulturelle Aspekte

Unternehmens-kultur

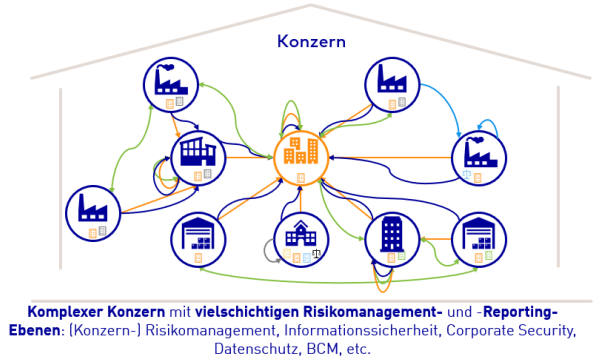
- Keine überschneidungsfreien Standards, Tools und Prozesse in Bereichen
- Zusammenarbeitsmodelle bereichsübergreifend noch nicht überall vollständig ausgeprägt

Persönliche Befindlichkeiten

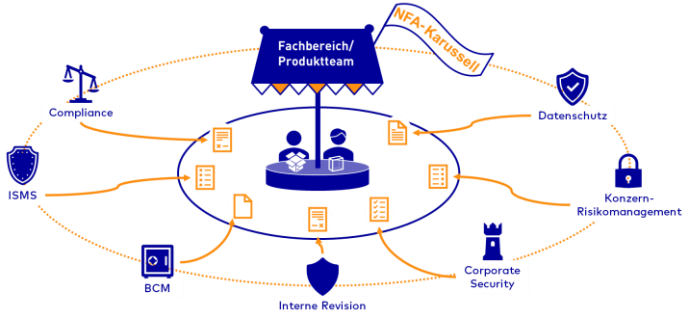
- „Bei uns ist das anders“
- Kein gemeinsamer Ansatz
- Historisch gewachsene Arbeitsabläufe

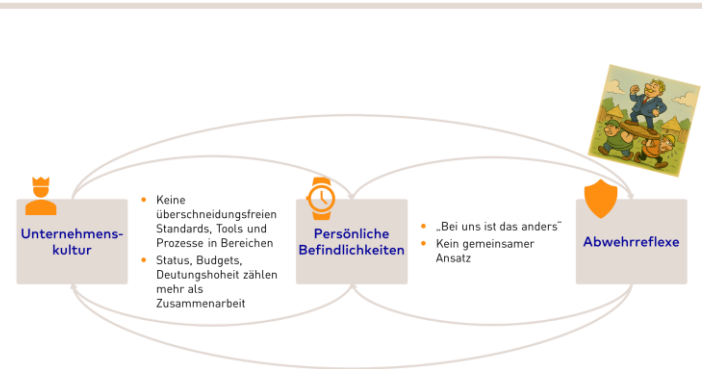
Abwehrreflexe

Ausgangslage – Zusammenfassung



Komplexer Konzern mit **vielschichtigen Risikomanagement-** und **-Reporting-Ebenen**: (Konzern-) Risikomanagement, Informationssicherheit, Corporate Security, Datenschutz, BCM, etc.





Kein konsistentes Gesamtbild

Belastung durch Mehrfacherhebungen (bspw. BIA, Schutzbedarf)

Konzernkultur und Silodenken erschweren Fokussierung auf Fachebene

BIA: Business Impact Analyse

Motivation für ein ganzheitliches Risikomanagement

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Aufwandsreduzierung – einmal erfassen, mehrfach nutzen

Vergleichbarkeit & **Priorisierung** über alle Disziplinen

Nachweise/Audits werden schlanker durch Standard-Bausteine

Regulatorik & Standards NIS2-konform, ISO 27001/22301; branchenspezifisch (B3S, SiKAT, TISAX).

Erwartung von Management & Vorstand: **konsolidiertes Risikobild** auf gemeinsamer Skala

Zukunftsfähige und flexible Struktur für effizientes Risiko-management mit Mehrwert

Harmonisierung – Kernelemente
Business ist Teil der Lösung

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Zentrale, erweiterbare Kataloge

- Konzernweit abgestimmte **Szenarien** und **Gefährdungen**
- **Anforderungen** und **Maßnahmen** mit sauberem **Mapping**, Ressource × Schutzziel × Eintrittswahrscheinlichkeit
- **Täterprofile** zur Einordnung der Eintrittswahrscheinlichkeit/Schadenshöhe

Rollen & Rhythmus

- Geklärte **RASCI-Rollen**, ISM, Risk Manager, BCM-Koordinator, Data Owner, Ressourcen- und Prozess**verantwortliche**
- Saubere **Governance-Anbindung**, Policies und Standards, Anschluss an ISMS und BCMS
- Verabredeter **Aktualisierungstakt**, jährlich und ereignisgetrieben, versionierte Katalog-**Releases**

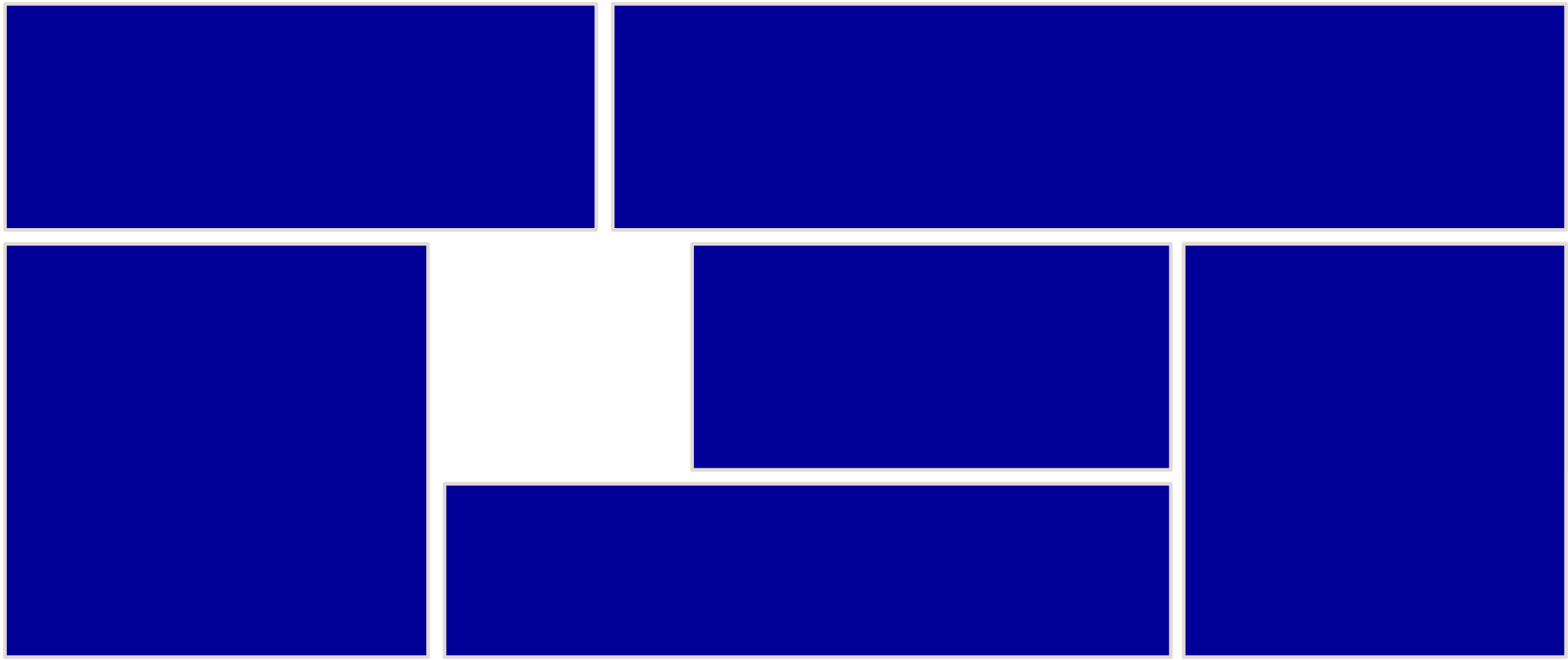
Gemeinsame Sprache & Basis

- **Eindeutige Begriffe**, Risiko, Informationswert/Datensatz, Ressource und Schutzbedarf
- Klar **abgestimmte Schutzziele**, Verfügbarkeit, Vertraulichkeit und Integrität
- **Gemeinsame Bewertungs-basis** und klarer **Scope**, Relevanzfilter & Wirkungs-kategorien, Kernprozesse und Kritikalität

Modulare Vertiefung möglich

- Andockbare **Domänenlayer,** B3S, SiKAT, TISAX und DORA, etc.
- **Werkzeugunabhängige** Umsetzung, gemeinsames **Datenmodell**, einheitliches Reporting
- Vorliegende **Zertifizierungen nutzen**, ISO 27001, B3S und ISO 22301 (BCMS) erleichtern Nachweise

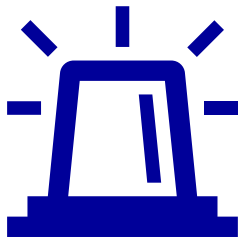
Typische Stolpersteine und kritische Erfolgsfaktoren



Typische Stolpersteine und kritische Erfolgsfaktoren

Tool First

„Dafür nutzen wir dann das ‚*Datenschutz3000*'-Tool, das hat bereits so hohe Lizenzkosten"



Typische Stolpersteine und kritische Erfolgsfaktoren

Fachlogik First

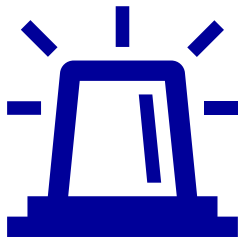
- Danach Erhebung Requirements (FA & NFA)
- Einheitliche Skalen im Tool abbilden
- Tools/Schnittstellen mappen

Typische Stolpersteine und kritische Erfolgsfaktoren

Fachlogik First
- Danach Erhebung Requirements (FA & NFA)
- Einheitliche Skalen im Tool abbilden
- Tools/Schnittstellen mappen

Silos und fehlende Einbindung

„Thomas vom ISMS-Policy-Team schreibt eine Richtline, die kann nächsten Monat veröffentlicht werden“



Typische Stolpersteine und kritische Erfolgsfaktoren

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

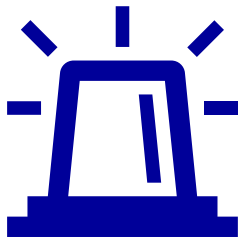
Fachlogik First
- Danach Erhebung Requirements (FA & NFA)
- Einheitliche Skalen im Tool abbilden
- Tools/Schnittstellen mappen

Stakeholder-Einbindung
- Alle an einen Tisch: ISMS, Datenschutz, BCM, Risikomanagement, Fachbereiche,…
- Inhalte gemeinsam erarbeiten (bspw. Policys)
- Wissen teilen (bspw. Glossar, Austauschformate)

Typische Stolpersteine und kritische Erfolgsfaktoren

Fachlogik First
- Danach Erhebung Requirements (FA & NFA)
- Einheitliche Skalen im Tool abbilden
- Tools/Schnittstellen mappen

Stakeholder-Einbindung
- Alle an einen Tisch: ISMS, Datenschutz, BCM, Risikomanagement, Fachbereiche,…
- Inhalte gemeinsam erarbeiten (bspw. Policys)
- Wissen teilen (bspw. Glossar, Austauschformate)



Methodenbrüche

„Klingt gut, wir nutzen aber weiterhin unsere Methode mit der XY-Skala.“

Typische Stolpersteine und kritische Erfolgsfaktoren

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Fachlogik First
- Danach Erhebung Requirements (FA & NFA)
- Einheitliche Skalen im Tool abbilden
- Tools/Schnittstellen mappen

Stakeholder-Einbindung
- Alle an einen Tisch: ISMS, Datenschutz, BCM, Risikomanagement, Fachbereiche,…
- Inhalte gemeinsam erarbeiten (bspw. Policys)
- Wissen teilen (bspw. Glossar, Austauschformate)

Einheitlichkeit
- Gemeinsame Kernstruktur (Szenario, Eintritt, Auswirkung)
- Verbindliche einheitliche Skalen
- Module andockbar (bei komplexerer Regulatorik)

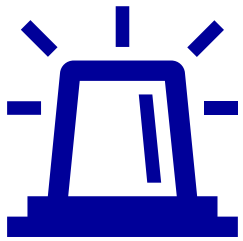
Typische Stolpersteine und kritische Erfolgsfaktoren

Fachlogik First
- Danach Erhebung Requirements (FA & NFA)
- Einheitliche Skalen im Tool abbilden
- Tools/Schnittstellen mappen

Unklarer Scope & Zielbild

„Wir fangen einfach mal an, die Fragen werden sich im Laufe des Projekts schon klären“

Stakeholder-Einbindung
- Alle an einen Tisch: ISMS, Datenschutz, BCM, Risikomanagement, Fachbereiche,…
- Inhalte gemeinsam erarbeiten (bspw. Policys)
- Wissen teilen (bspw. Glossar, Austauschformate)



Einheitlichkeit
- Gemeinsame Kernstruktur (Szenario, Eintritt, Auswirkung)
- Verbindliche einheitliche Skalen
- Module andockbar (bei komplexerer Regulatorik)

Typische Stolpersteine und kritische Erfolgsfaktoren

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Fachlogik First
- Danach Erhebung Requirements (FA & NFA)
- Einheitliche Skalen im Tool abbilden
- Tools/Schnittstellen mappen

Verbindliche Definition Scope
- Zielbild & Scope verbindlich definieren
- Kernprozesse/Kritikalität klären
- Einheitliches Vokabular definieren
- Pilot & Iterationen: kleinere Releases zur Korrektur nach Feedback

Stakeholder-Einbindung
- Alle an einen Tisch: ISMS, Datenschutz, BCM, Risikomanagement, Fachbereiche,…
- Inhalte gemeinsam erarbeiten (bspw. Policys)
- Wissen teilen (bspw. Glossar, Austauschformate)

Einheitlichkeit
- Gemeinsame Kernstruktur (Szenario, Eintritt, Auswirkung)
- Verbindliche einheitliche Skalen
- Module andockbar (bei komplexerer Regulatorik)

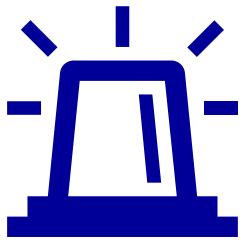
Typische Stolpersteine und kritische Erfolgsfaktoren

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Fachlogik First
- Danach Erhebung Requirements (FA & NFA)
- Einheitliche Skalen im Tool abbilden
- Tools/Schnittstellen mappen

Verbindliche Definition Scope
- Zielbild & Scope verbindlich definieren
- Kernprozesse/Kritikalität klären
- Einheitliches Vokabular definieren
- Pilot & Iterationen: kleinere Releases zur Korrektur nach Feedback

Stakeholder-Einbindung
- Alle an einen Tisch: ISMS, Datenschutz, BCM, Risikomanagement, Fachbereiche,…
- Inhalte gemeinsam erarbeiten (bspw. Policys)
- Wissen teilen (bspw. Glossar, Austauschformate)



Einheitlichkeit
- Gemeinsame Kernstruktur (Szenario, Eintritt, Auswirkung)
- Verbindliche einheitliche Skalen
- Module andockbar (bei komplexerer Regulatorik)

Ungeklärte Rollen

„Dafür ist doch BCM verantwortlich! … oder doch der Fachbereich? Wir jedenfalls nicht….“

Typische Stolpersteine und kritische Erfolgsfaktoren

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Fachlogik First

- Danach Erhebung Requirements (FA & NFA)
- Einheitliche Skalen im Tool abbilden
- Tools/Schnittstellen mappen

Verbindliche Definition Scope

- Zielbild & Scope verbindlich definieren
- Kernprozesse/Kritikalität klären
- Einheitliches Vokabular definieren
- Pilot & Iterationen: kleinere Releases zur Korrektur nach Feedback

Stakeholder-Einbindung

- Alle an einen Tisch: ISMS, Datenschutz, BCM, Risikomanagement, Fachbereiche,…
- Inhalte gemeinsam erarbeiten (bspw. Policys)
- Wissen teilen (bspw. Glossar, Austauschformate)

Einheitlichkeit

- Gemeinsame Kernstruktur (Szenario, Eintritt, Auswirkung)
- Verbindliche einheitliche Skalen
- Module andockbar (bei komplexerer Regulatorik)

Rollen und Verantwortlichkeiten

- RASCI etablieren
- Benannte Owner: Prozess, Ressource, Information, …
- Governance-Struktur für Abstimmung & Eskalation

RASCI: Responsible, Accountable, Support, Consulted, Informed

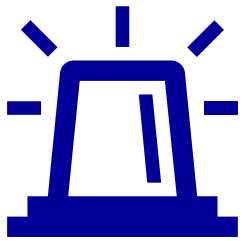
Typische Stolpersteine und kritische Erfolgsfaktoren

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Fachlogik First
- Danach Erhebung Requirements (FA & NFA)
- Einheitliche Skalen im Tool abbilden
- Tools/Schnittstellen mappen

Verbindliche Definition Scope
- Zielbild & Scope verbindlich definieren
- Kernprozesse/Kritikalität klären
- Einheitliches Vokabular definieren
- Pilot & Iterationen: kleinere Releases zur Korrektur nach Feedback

Stakeholder-Einbindung
- Alle an einen Tisch: ISMS, Datenschutz, BCM, Risikomanagement, Fachbereiche,…
- Inhalte gemeinsam erarbeiten (bspw. Policys)
- Wissen teilen (bspw. Glossar, Austauschformate)



Einheitlichkeit
- Gemeinsame Kernstruktur (Szenario, Eintritt, Auswirkung)
- Verbindliche einheitliche Skalen
- Module andockbar (bei komplexerer Regulatorik)

Rollen und Verantwortlichkeiten
- RASCI etablieren
- Benannte Owner: Prozess, Ressource, Information, …
- Governance-Struktur für Abstimmung & Eskalation

Reporting-Flickenteppich

„Jeder Bereich, Tochterunternehmen reportet in einem eigenen Format und eigener Struktur.“

RASCI: Responsible, Accountable, Support, Consulted, Informed

Typische Stolpersteine und kritische Erfolgsfaktoren

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Fachlogik First

- Danach Erhebung Requirements (FA & NFA)
- Einheitliche Skalen im Tool abbilden
- Tools/Schnittstellen mappen

Verbindliche Definition Scope

- Zielbild & Scope verbindlich definieren
- Kernprozesse/Kritikalität klären
- Einheitliches Vokabular definieren
- Pilot & Iterationen: kleinere Releases zur Korrektur nach Feedback

Stakeholder-Einbindung

- Alle an einen Tisch: ISMS, Datenschutz, BCM, Risikomanagement, Fachbereiche,…
- Inhalte gemeinsam erarbeiten (bspw. Policys)
- Wissen teilen (bspw. Glossar, Austauschformate)

Einheitlichkeit

- Gemeinsame Kernstruktur (Szenario, Eintritt, Auswirkung)
- Verbindliche einheitliche Skalen
- Module andockbar (bei komplexerer Regulatorik)

Konsolidierung Reporting

- Einheitliches Layout und Zyklen für alle
- Gemeinsame Datenbasis/APIs
- Release-Rhythmus: versionierte Kataloge, Templates

Rollen und Verantwortlichkeiten

- RASCI etablieren
- Benannte Owner: Prozess, Ressource, Information, …
- Governance-Struktur für Abstimmung & Eskalation

RASCI: Responsible, Accountable, Support, Consulted, Informed

Nutzen und Mehrwert

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Weniger **Analyse- & Umsetzungsaufwand** durch **zentral** definierte **Methodenelemente**

Höhere **Verlässlichkeit** bei Audits/Nachweisen dank **standardisierter Maßnahmen & Rollen**

Einfachere Schutzbedarfs- & Risikobewertung durch konsistente **Bewertungslogik**

Modular **adaptierbar** für branchenspezifische Tiefen (z. B. SiKAT, B3S, TISAX) – ohne Bruch im Reporting.

Konsistenz & Anschlussfähigkeit in bestehenden Governance- und Toolstrukturen.

Vielen Dank!

Patrick Hesse
Senior Manager Informationssicherheit (TISP)

IT Strategie & Steuerung (C-TISS)
Durlacher Allee 93
76131 Karlsruhe

Mobil +49 15121963827
p.hesse@enbw.com

Katharina Otto
Information Security Manager (TISP)

IT Security Steuerung (C-TICS)
Durlacher Allee 93
76131 Karlsruhe

Mobil +49 16099192247
k.otto@enbw.com