F24 Experience Tour München

F24

GRC in der Praxis:
Vernetzung von Informationssicherheit und BCM

Public

Vorstellung:
Ihre Referenten

Timo Lutzenberger
F24 AG
Head of Sales & Marketing GRC
timo.lutzenberger@f24.com

Patrick Bieg
ThiemeBieg & Associates GmbH
Geschäftsführer
patrick.bieg@thiemebieg.com

Aktuelle Bedrohungslage im Cyberraum

Fakten und Zahlen

8 von 10

Unternehmen sind von Datendiebstahl, Spionage oder Sabotage betroffen

Quelle: Bitkom

58%

der Cyberschäden entstehen durch Ransomeware - Angriffe

Quelle: Cyber Security Resilience 2024

43 %

der Notfallkrisenpläne wurden aufgrund von Cybersicherheitsvorfällen und Datenschutzverletzungen aktiviert.

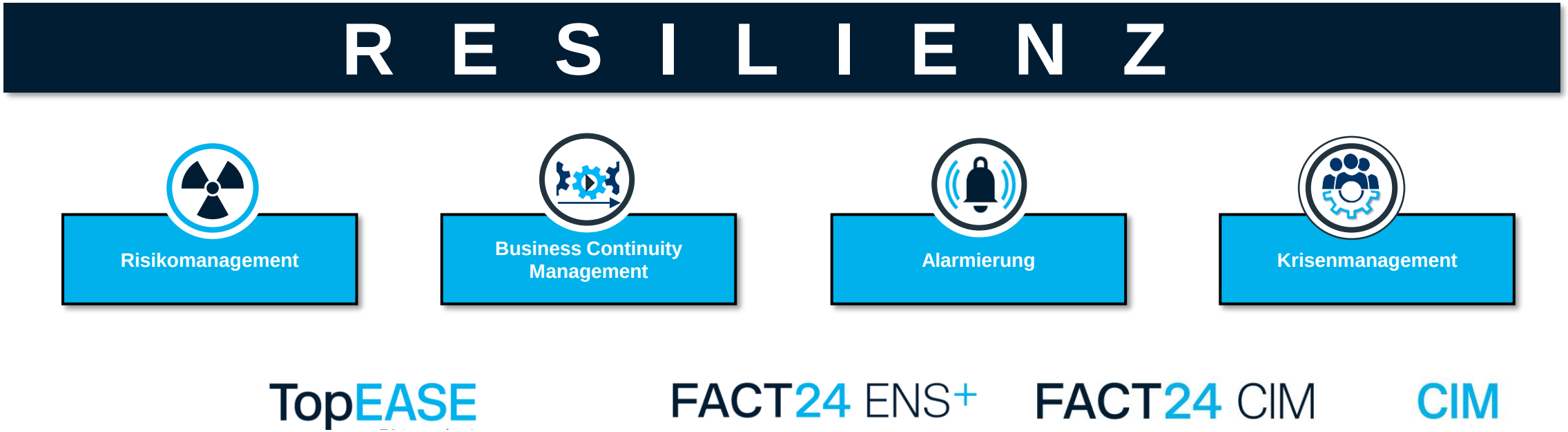
Quelle: BCI ECC Report 2025

> 266,6 Milliarden Euro

resultieren aus den analogen und digitalen Cyber-Angriffen.

Quelle: Bitkom

Unsere Lösungen unterstützen Sie in allen Bereichen der Resilienz.



2024: Prägende Ereignisse

Autoindustrie in der Krise

Tesla Brandanschlag

Crowdstrike Outage

Ampel-Aus & Trump-Sieg

Cyber-Angriff Starbucks Software-Lieferant

DORA Anwendungsfrist

Q1 | **Q2** | **Q3** | **Q4** | **2025**

Hacker-Bedrohung aus Russland und China

Veröffentlichung der Causa Microsoft

Jahrhundert-hochwasser

NIS2 & Lieferkettengesetz

Lieferkettenunterbrechung durch Hafenstreiks

Mgmt Haftbarkeit Südwestfalen-IT-Vorfall

Der CrowdStrike Vorfall

Der CrowdStrike Vorfall

Was ist passiert?

- Ein von CrowdStrike verteiltes Update verursachte in Windows-Systemen einen kritischen Speicherfehler. Dadurch stürzte Windows während des Bootvorgangs mit einem „Blue Screen of Death“ (BSOD) ab und war danach in einer Endlosschleife von Absturz und Neustart gefangen.
- Dieses Update führte zu weltweiten IT-Ausfällen. Das Bundesamt für Sicherheit in der Informationstechnik stufte den Vorfall auf der 4-stufigen Skala auf Stufe 3/Orange ein.

Auswirkungen:

- Unternehmen weltweit erlebten erhebliche Betriebsunterbrechungen, die zu finanziellen Verlusten führten. Flughäfen mussten Flüge streichen, Krankenhäuser Operationen verschieben, und IT-Riesen wie Microsoft waren betroffen.
- Regulierungsbehörden wie das BSI planen Maßnahmen, um zukünftige Vorfälle zu verhindern, was zusätzliche Kosten und Anforderungen für Unternehmen bedeutet.

F24

NIS2-Richtlinie

NIS2 - Die EU-weite Gesetzgebung zur Cybersicherheit

Was ist NIS2?

Die Richtlinie zur Netz- und Informationssicherheit sieht rechtliche Maßnahmen vor, um das allgemeine Niveau der Cybersicherheit in der EU zu erhöhen und mehr Branchen vor Cyberbedrohungen zu schützen.

Was sind die gesetzlichen Vorgaben?

- Berichterstattung über Vorfälle
- Handhabung von Schwachstellen
- Risikomanagement
- Entwicklung von Reaktions- und Wiederherstellungsmaßnahmen
- Beaufsichtigung und Durchführung

F24

GRC Plattform TopEase®

TopEase® Module

TopEASE
ein F24 Produkt

Risiko [NFR]

Risikobewertung via Fragenkatalog, Echtzeit Risikolage, Definition von Maßnahmen zur Risikoreduktion

Business Continuity [BCM/BIA]

Abbildung von Unternehmensstrukturen und Abhängigkeiten, Notfall- und Kontinuitätsplanung

Asset [EAM]

Asset-Management, Visualisierungen, Governance-Dokumentation, Simulation von Architektur-Szenarien

Sicherheit [SOA/ISMS]

Security Assessment, integriertes Sicherheitsmanagement, Sicherheits-Compliance, Erstellung und Verteilung von Fragenkatalogen

Regulation

Implementierung regulatorischer Vorgaben, GAP-Analyse, Betroffenheits- und Auswirkungs-Analysen

Prozess [BPM]

Prozessdokumentation, Prozessvisualisierung, Automatisierung und Optimierung von Wertschöpfungsketten

Resilienz

Resilienzüberwachung, Risikoüberwachung, Prozessüberwachung, Maßnahmensteuerung

Kontrolle [IKS]

Kontrollsysteme, Compliance Assessment, strukturiertes Kontrollmanagement für unterschiedliche Zielgruppen und Themen

Transformation

Pflege und Bewertung von Veränderungen, Portfolio und Multi-Projekt-Management

Beherrschen Sie die Komplexität Ihrer Organisation einfach und professionell mit unserer GRC-Plattform TopEase®.

Asset Dokumentation

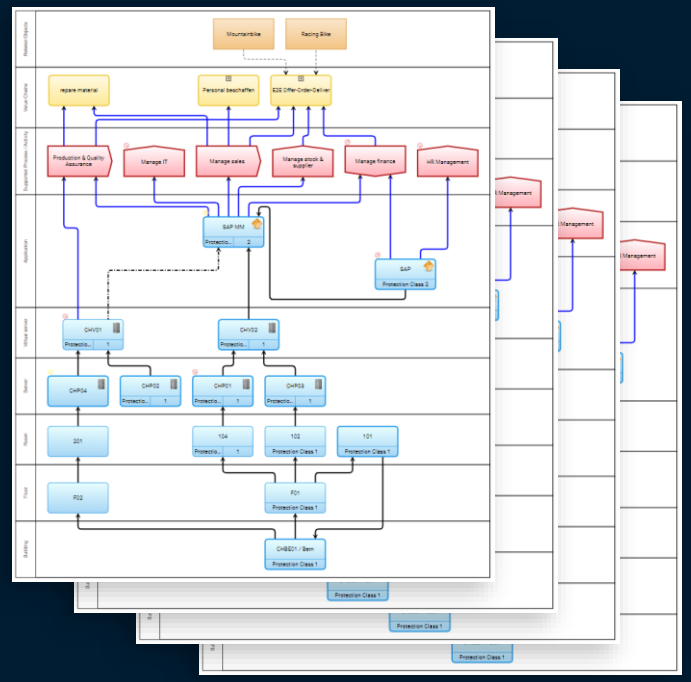
Gebäude

Infrastruktur

Applikation

Prozesse

Digital Twin



TopEASE
an F24 product

1. Wir bringen alle Geschäftsprozesse und Aktivitäten auf eine Übersicht und erstellen einen digitalen Zwilling
2. Auf Basis des digitalen Zwillings zeigen wir alle möglichen Vulnerabilitäten auf
3. Mit TopEase bauen wir Tools um die Vernetzung dieser Prozesse zu verstehen.

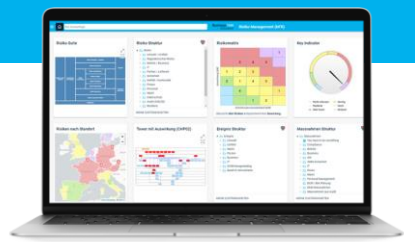
Architektur: Aufbau von TopEase®

F24

TopEase®
GRC Solutions

TopEase®
Platform

TopEase®
Integration



- Process / Asset
- BCM/BIA
- Security/ ISMS
- IKS
- Risk [NFR]
- DORA

- Reporting
- Rollen / Rights
- Workflow
- Method / Concept
- Repository

- Process Tool BPMN
- Monitoring
- CMDB
- List of Location
- HR Tool (SAP HR)

F24

Use Case: Vernetzung von Informationssicherheit und BCM

TopEASE

TopEase®
Demand Management

- TopEase® Anforderungsmanagement
- TopEase® Solution und Landscape-Architektur
- Proof of Concept

TopEase®
Implementierung

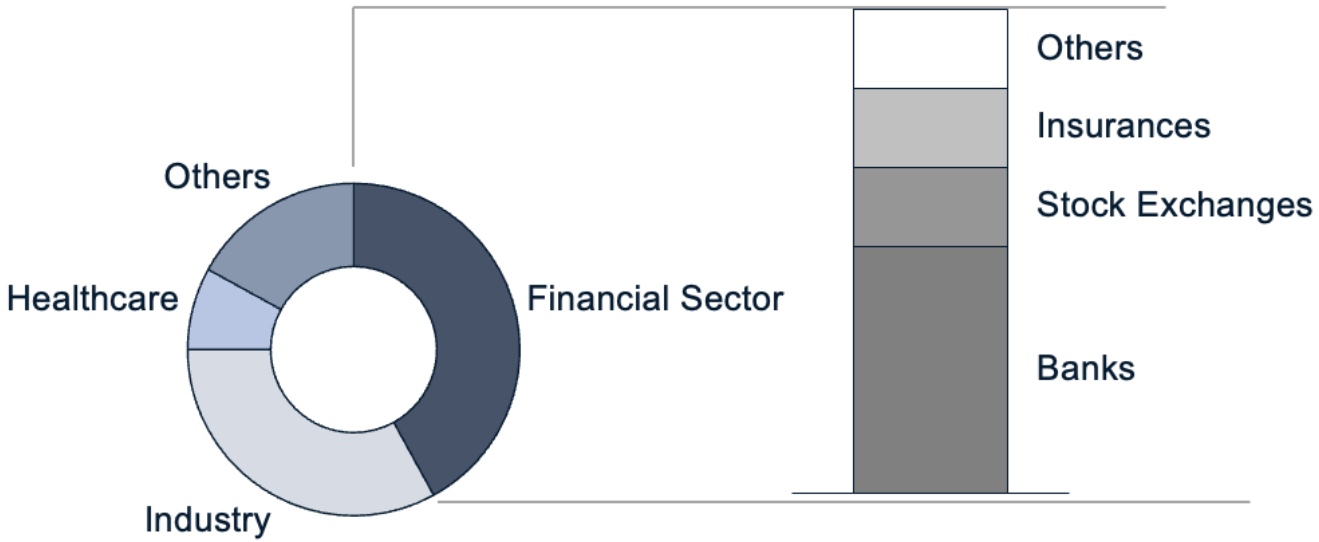
- Projekt Management und Implementierung
- Technische Beratung und EAM Support
- Model Design

TopEase®
Service & Betrieb

- Hybrid & on-demand competence center
- GRC Consulting
- Projekt Support (z.B. während Zertifizierungen, Audits)

ThiemeBieg & Associates – ihr verlässlicher Partner im Regulatorikbereich

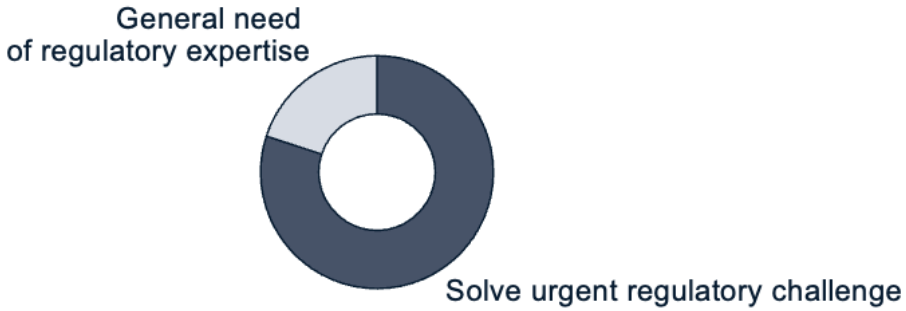
Customers by Sector



Main consulting areas (by GRC topic)

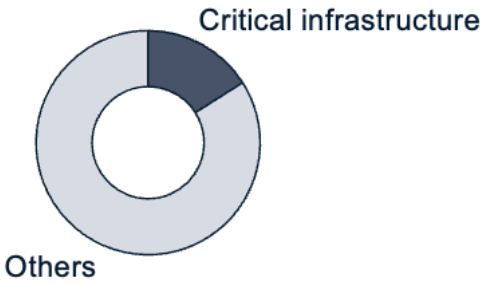
Data: 2023, only active clients, sub-entities are not counted separately

Reasons for new engagement with ThiemeBieg (est.)



Global Perspective

Critical Infrastructure



Situation im Unternehmen

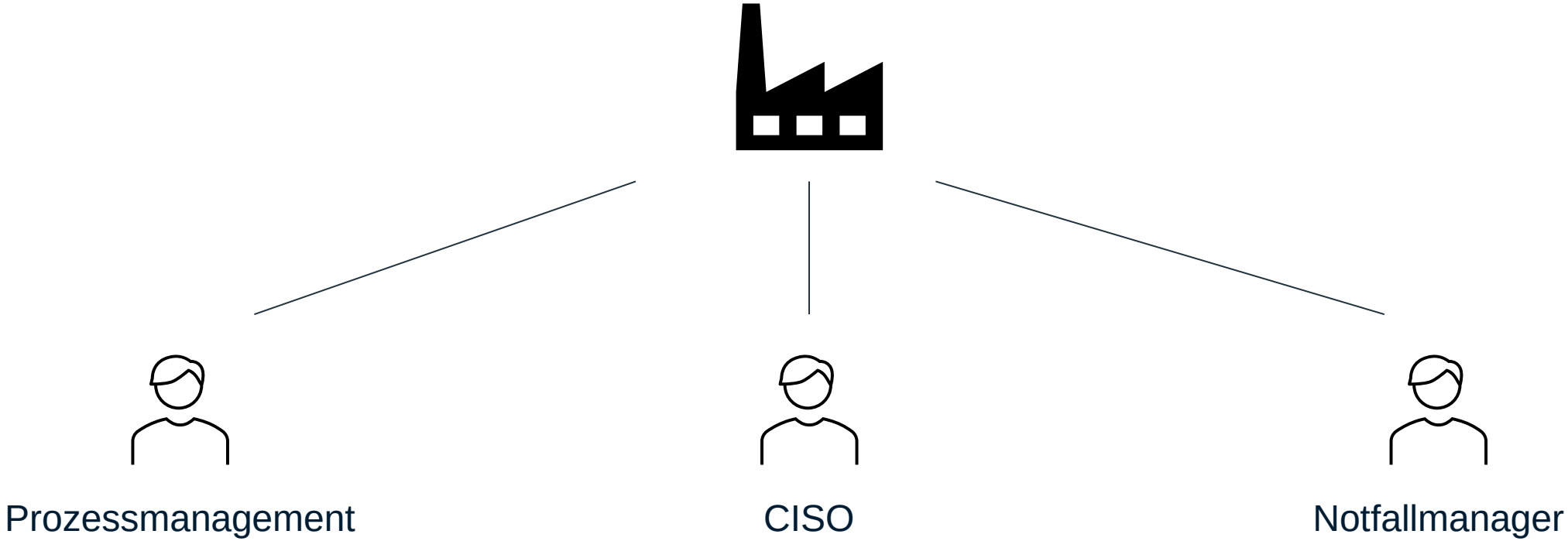
“wir haben bereits Informationssicherheit und Kontinuitätsmanagement umgesetzt.“

TopEase:

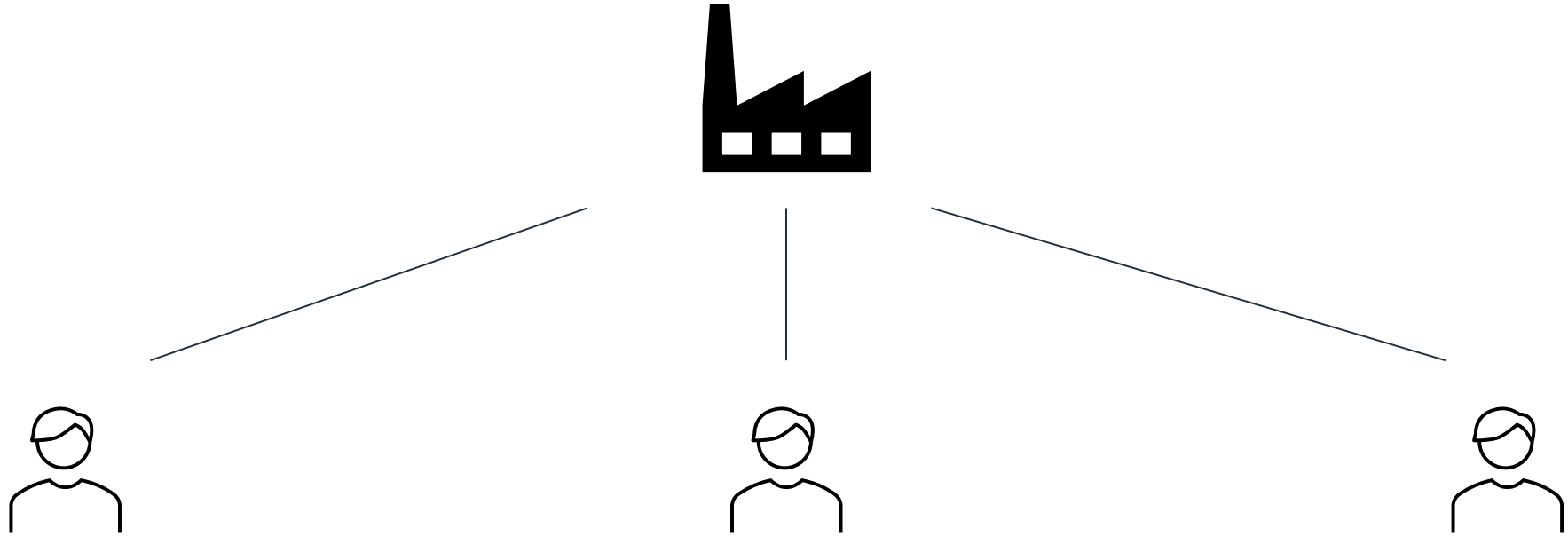
100% Compliance.
-30% Kosten.[1]

1 Expertenschätzung auf Basis von realen Umgebungen und Ergebnissen, bei Ablösung mehrerer Einzel-Solutions und Wechsel auf TopEase.

Ist-Situation:
Verteile Bebauung im GRC Bereich



Ist-Situation:
Verteile Bebauung im GRC Bereich



Prozessmanagement

Prozesse

- SfO / Prozesslandschaft
- Beziehungen Prozesse / Assets

CISO

SBF / SoA

- Integrität, Vertraulichkeit
- Sicherheitskontrollen

Notfallmanager

BIA

- Verfügbarkeit
- Geschäftsfortführungsplanung

Problemstellung:
Verteilte Systeme für vernetzte Tätigkeiten

Prozesse

- SfO / Prozesslandschaft
- Beziehungen Prozesse / Assets

SBF / SoA

- Integrität, Vertraulichkeit
- Sicherheitskontrollen

BIA

- Verfügbarkeit
- Geschäftsfortführungsplanung

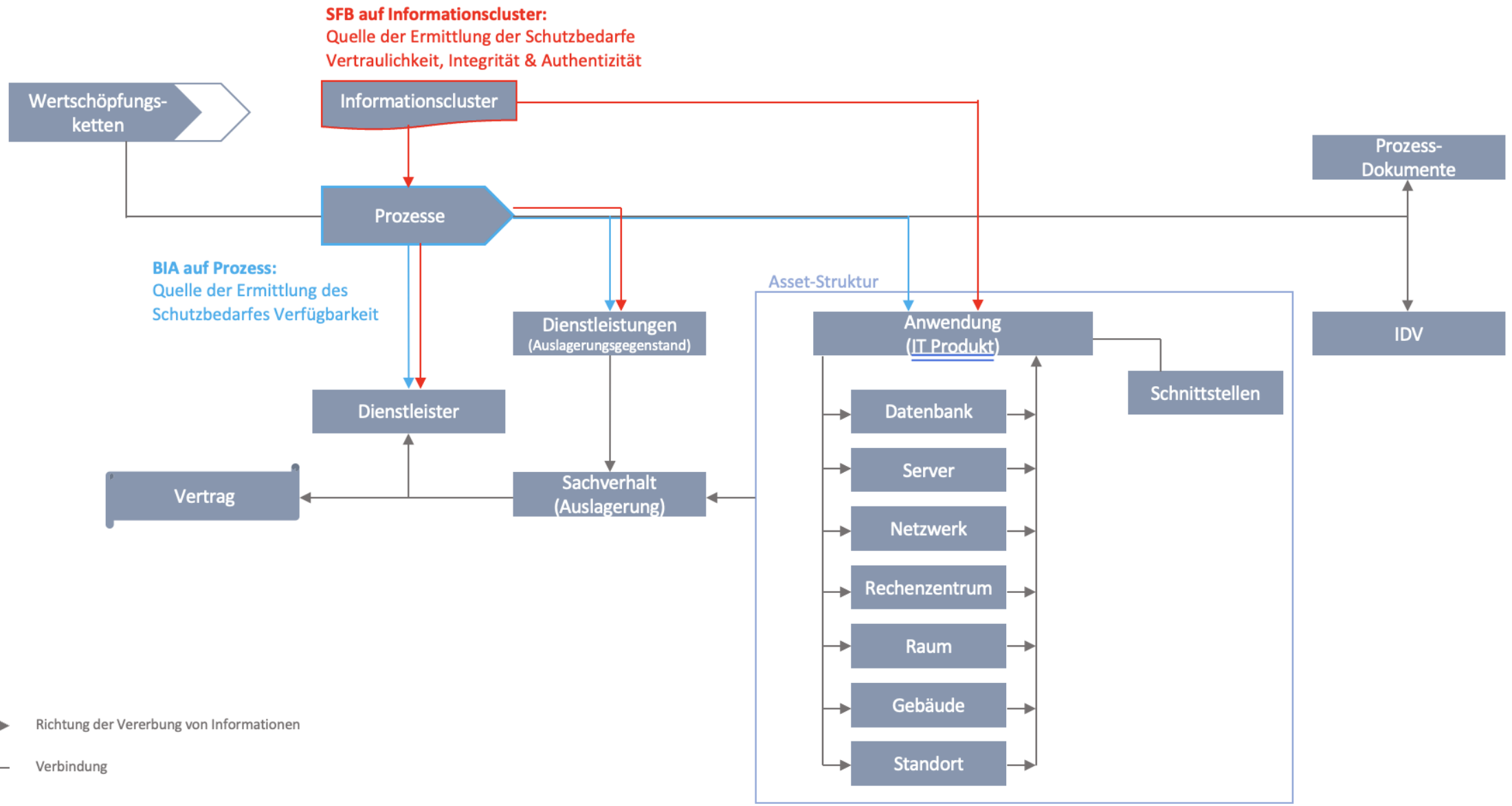
Übliche Schwachpunkte aus Sicht der regulatorischen Aufsicht (z.B. BaFin):

- Kein **einheitlicher** und **vollständiger Informationsverbund**
- Unterschiedliche Prozess-Datenbasis (2 bis mehrere „Prozesshäuser“, jeweils auf Use-Case adaptiert)
- Unterschiedliche Asset-Landschaften, insb. Abweichung zw. Prozessen, IT-Sicherheit, BCMS

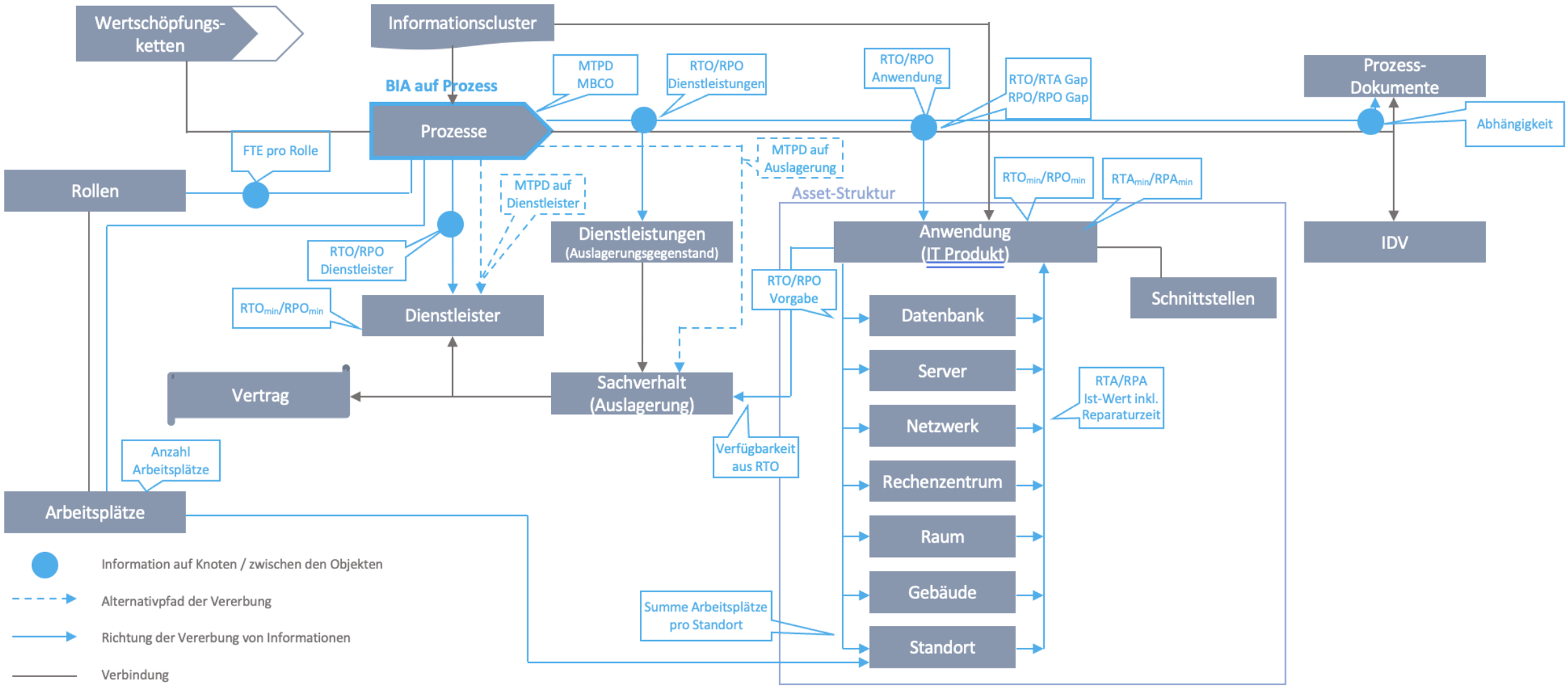
Schwachpunkte aus Business-Sicht:

- **Keine Datendurchgängigkeit (woher kommen Vererbungen?)**
- Prozessuale changes, z.B. neue Verfahren nach DORA betreffen alle Einzellösungen, bedingen Schnittstellenänderungen etc. (kostenintensiv, langwierig, hohe Abstimmbedarfe)
- Inhaltliche Changes (z.B. Change in Asset-Struktur) kommen mit Verzug oder unvollständig in Einzellösungen an

Darstellung des Informationsverbundes mit Ermittlung und Vererbung der Schutzbedarfe (oberste Ebene)



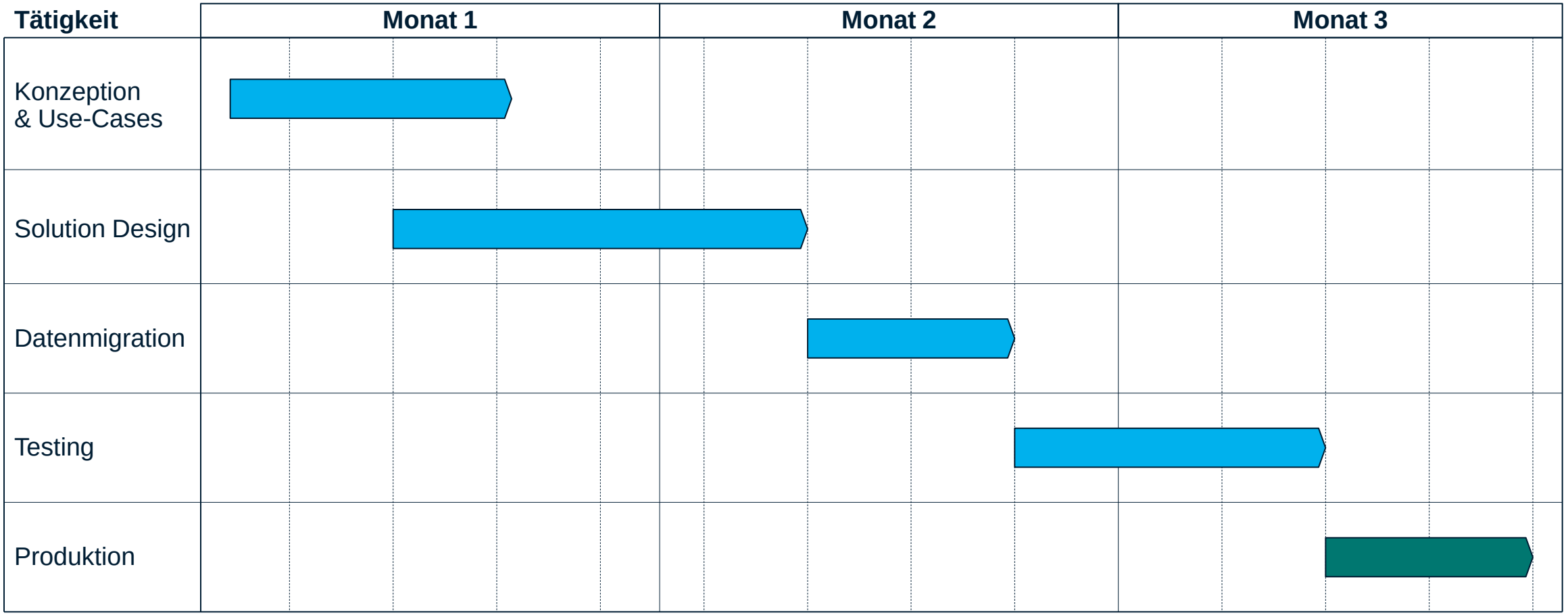
Erweitertes Informationsverbundmodell aus BIA-Sicht mit Ermittlung und Vererbung von Informationen inkl. ITSCM



Zielbild TopEase GRC

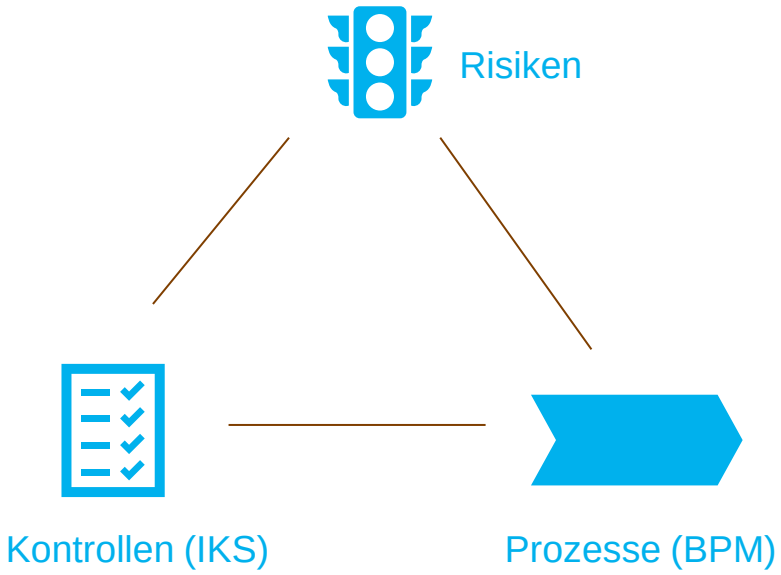
Gleiche Datenbasis, unterschiedliche Sichtweisen auf die Daten:
„Compliance **hoch**, Kosten **runter**“

Einführung von TopEase – in unter 100 Tagen zum Erfolg



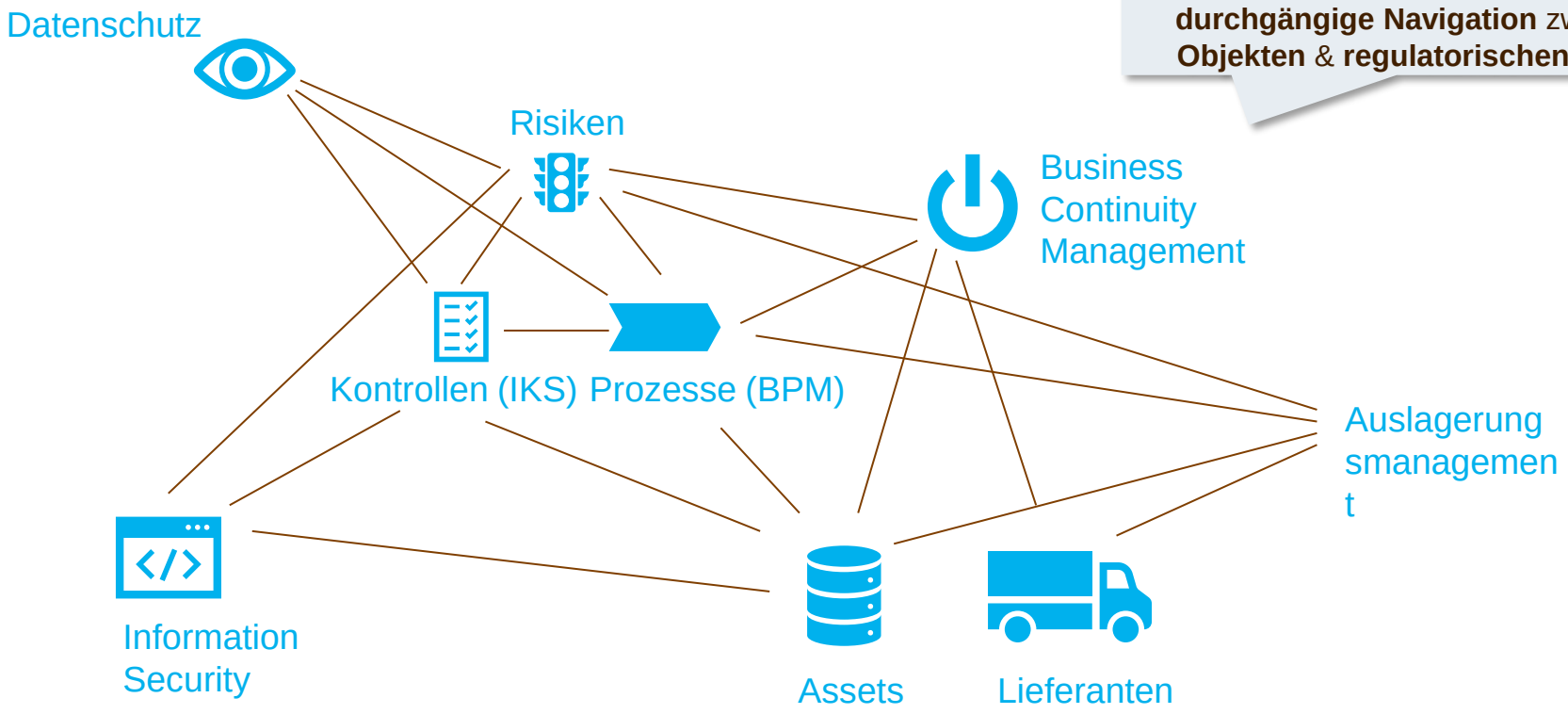
Prämisse: Nutzungen der Solutions im Standard und mittels Standardkonfigurationen von TB&A, Verfügbarkeiten (Kunden, TB&A, F24) vorausgesetzt

Grundkonstrukt von TopEase – regulatorischer Dreiklang

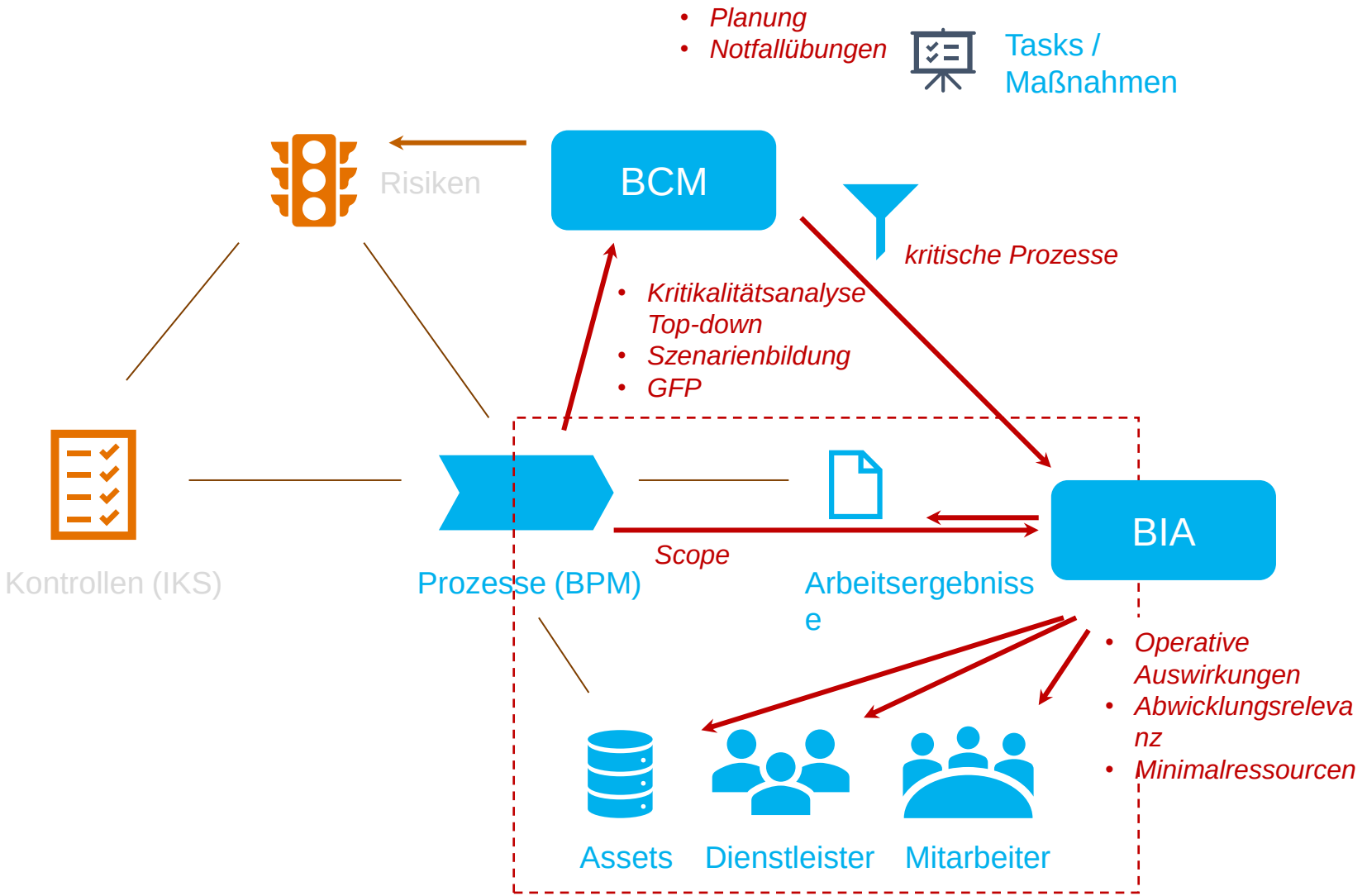


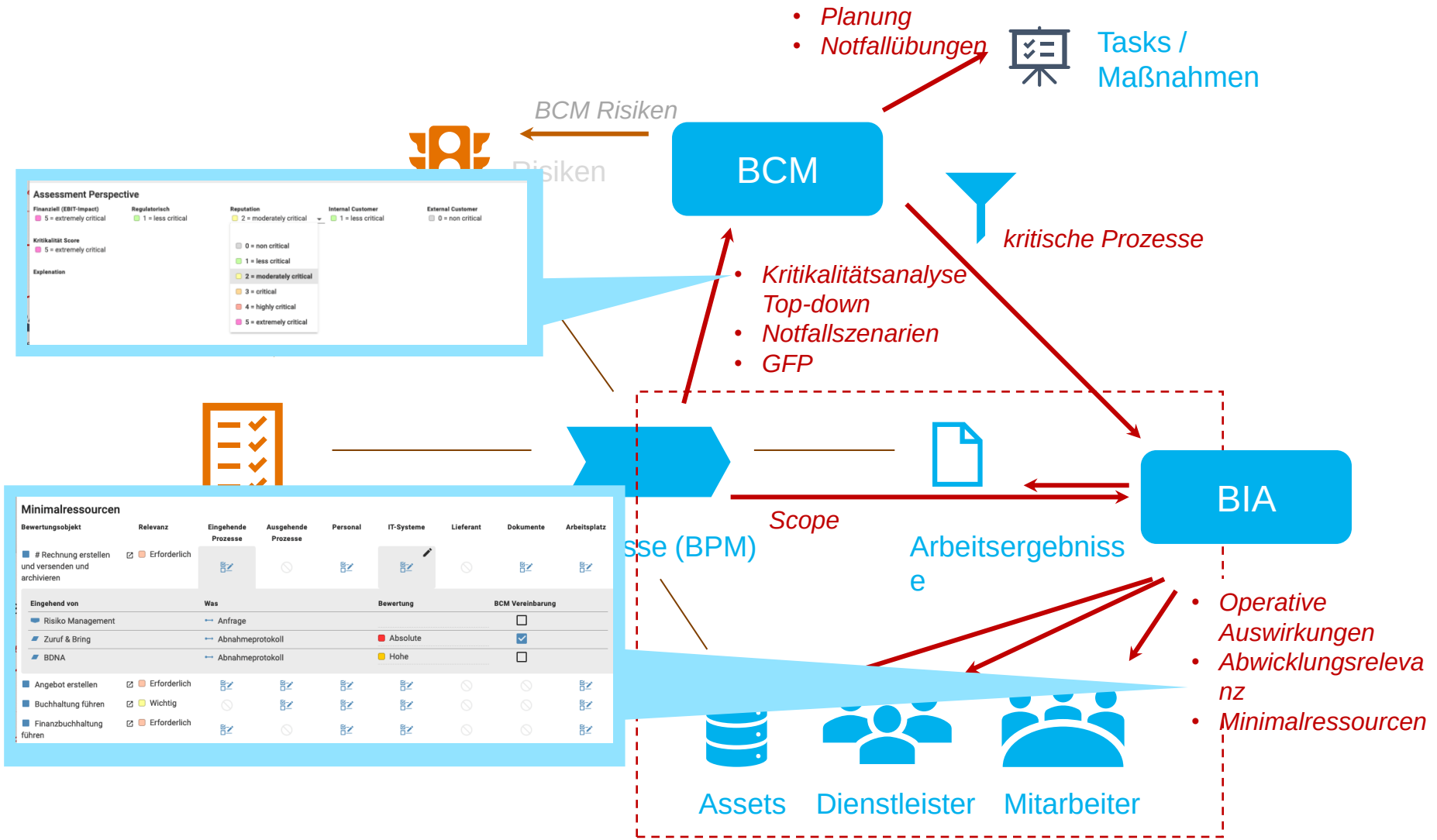
Erweiterung des Konstruktes je Use-Case

Abbildung des gesamten **regulatorisch relevanten Informationsverbundes** innerhalb des TopEase Datenmodells - **durchgängige Navigation** zwischen den **Objekten** & **regulatorischen** Use-Cases



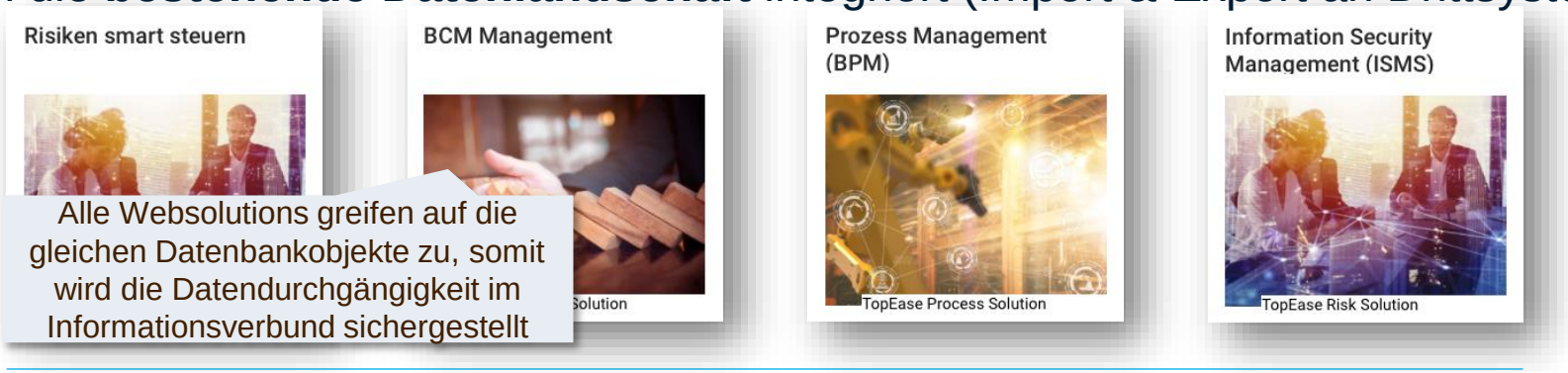
Pro Use-Case können alle Tätigkeiten durchgeführt werden




• Planung
• Notfallübungen
Tasks / Maßnahmen
BCM Risiken
BCM
kritische Prozesse
• Kritikalitätsanalyse Top-down
• Notfallszenarien
• GFP
Assessment Perspective
Minimalressourcen
Scope
BIA
Arbeitsergebnisse
• Operative Auswirkungen
• Abwicklungsrelevanz
• Minimalressourcen
Assets
Dienstleister
Mitarbeiter

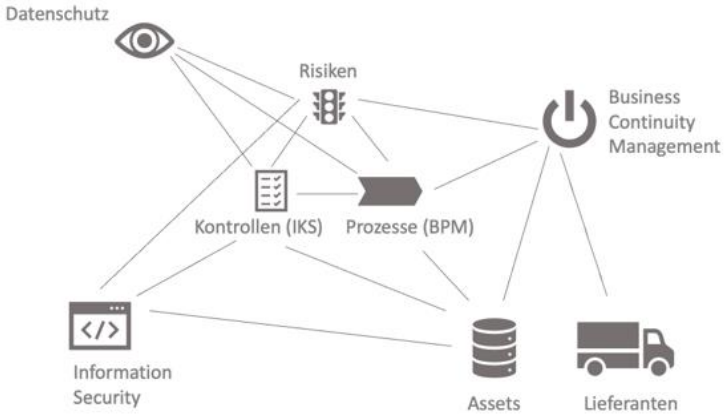
Aufbau der TopEase Plattform – die **Solutions** stellen jeweils **einen GRC Use-Case** dar, über die **Plattform** wird TopEase in die **bestehende Datenlandschaft** integriert (Import & Export an Drittsysteme)

Solutions



Alle Websolutions greifen auf die gleichen Datenbankobjekte zu, somit wird die Datendurchgängigkeit im Informationsverbund sichergestellt

Plattform



Die Vernetzung der einzelnen Objekte findet auf Plattformebene in einem Repository statt

Authentifizierung[1]

Microsoft Entra ID

okta

Systemanbindung[1]

Jira

SAP HCM

Technische Importfo[1]

Excel

CSV

{ REST }

BPMN

<xml />

Technische mate[1]

BPMN

PDF

CSV

W

Excel

{ REST }

<xml />

Anbindung BI-Tools[1]

JDBC

+ableau

What‘s next?

Abschätzung der Vorteile für Ihre Landschaft mittels der TopEase Potentialanalyse:

- Prüfung Ist-Situation Bebauung
- Prüfung Ist-Situation regulatorische Compliance
- Erstellung TopEase Architekturentwurf

Q & A

Vielen Dank für Ihre Aufmerksamkeit!

F24

F24 AG | Ridlerstraße 57 | 80339 München | Deutschland
T +49 89 23 23 638 0 | F +49 89 23 23 638 6 | office@f24.com
www.f24.com